



고가용성(페일오버)

다음 주제에서는 threat defense 시스템의 고가용성을 달성하기 위해 액티브/스탠바이 페일오버를 컨피그레이션하고 관리하는 방법을 설명합니다.

- [고가용성\(페일오버\) 정보, 1 페이지](#)
- [고가용성을 위한 시스템 요구 사항, 10 페이지](#)
- [고가용성에 대한 지침, 12 페이지](#)
- [고가용성 구성, 13 페이지](#)
- [고가용성 관리, 27 페이지](#)
- [고가용성 모니터링, 37 페이지](#)
- [고가용성 트러블슈팅\(페일오버\), 40 페이지](#)

고가용성(페일오버) 정보

고가용성 또는 페일오버 설정에서는 두 디바이스가 조인하므로 기본 디바이스에 장애가 발생하면 보조 디바이스가 대신 작동할 수 있습니다. 그러면 디바이스 장애 시 네트워크를 계속 운영하는 데 도움이 됩니다.

고가용성을 컨피그레이션하려면 2개의 동일한 threat defense 디바이스가 전용 페일오버 링크와 선택 사항인 상태 링크를 통해 서로 연결되어 있어야 합니다. 두 유닛은 페일오버 링크를 통해 지속적으로 통신하면서 각 유닛의 작동 상태를 확인하고 구축된 컨피그레이션 변경 사항을 동기화합니다. 시스템은 상태 링크를 사용해 연결 상태 정보를 스탠바이 디바이스에 전달하므로, 페일오버가 발생할 경우 사용자 연결이 유지됩니다.

두 유닛은 액티브/패시브 쌍을 이루는데, 여기서 하나는 액티브 유닛이며 트래픽을 전달합니다. 스탠바이 유닛은 능동적으로 트래픽을 전달하지 않지만, 액티브 유닛에서 컨피그레이션 및 기타 상태 정보를 동기화합니다.

액티브 유닛의 상태(하드웨어, 인터페이스, 소프트웨어 및 환경 상태)를 모니터링하여 특정 페일오버 조건이 충족되는지 확인합니다. 페일오버 조건이 충족되면 액티브 유닛은 스탠바이 유닛으로 페일오버를 시작하며, 이때 스탠바이 유닛이 액티브 유닛이 됩니다.

액티브/스탠바이 페일오버 정보

액티브/스탠바이 페일오버에서는 스탠바이 위협 방지 디바이스를 사용해 장애가 발생한 유닛의 기능을 인수할 수 있습니다. 액티브 유닛에 장애가 발생하는 경우 스탠바이 유닛이 액티브 유닛이 됩니다.

기본/보조 역할 및 액티브/스탠바이 상태

페일오버 쌍의 두 유닛의 주된 차이점은 어느 유닛이 액티브 유닛이고 어느 유닛이 스탠바이 유닛인지와 관련 있습니다. 즉, 어떤 IP 주소를 사용하고 어떤 유닛이 트래픽을 능동적으로 전달하는지에 달려 있습니다.

그러나 유닛 간의 몇몇 차이점은 어느 유닛이 기본(컨피그레이션에 지정된 사항에 따라) 유닛이고 어느 유닛이 보조 유닛인지에 따라서도 결정됩니다.

- 두 유닛이 동시에 시작되고 둘 다 정상적인 상태로 작동될 경우 기본 유닛은 항상 액티브 유닛이 됩니다.
- 기본 유닛의 MAC 주소는 액티브 IP 주소와 항상 연계됩니다. 보조 유닛이 액티브 유닛이 되고 페일오버 링크를 통해 기본 유닛의 MAC 주소를 획득할 수 없는 경우에는 이러한 규칙에 예외가 발생합니다. 이 경우 보조 유닛의 MAC 주소가 사용됩니다.

시작 시 액티브 유닛 결정

액티브 유닛은 다음에 따라 결정됩니다.

- 유닛이 부팅되고 이미 액티브로 실행 중인 피어가 감지된 경우, 해당 유닛은 스탠바이 유닛이 됩니다.
- 유닛이 부팅되고 피어가 감지되지 않은 경우 해당 유닛은 액티브 유닛이 됩니다.
- 두 유닛이 동시에 부팅될 경우 기본 유닛이 액티브 유닛이 되고 보조 유닛은 스탠바이 유닛이 됩니다.

페일오버 이벤트

액티브/스탠바이 페일오버 시 페일오버는 유닛을 기준으로 실행됩니다.

다음 표에서는 각 페일오버 이벤트에 대한 페일오버 작업을 보여줍니다. 이 표에는 각 페일오버 이벤트에 적용되는 페일오버 정책(페일오버 실행 또는 페일오버 없음), 액티브 유닛에서 시행한 조치, 스탠바이 유닛에서 시행한 조치, 페일오버 조건 및 각 조치에 대한 특별 참고 사항이 나와 있습니다.

표 1: 페일오버 이벤트

오류 이벤트	정책	액티브 유닛 조치	스탠바이 유닛 조치	참고
액티브 유닛 오류(전력 또는 하드웨어)	페일오버	해당 없음	액티브 상태가 됨 액티브가 실패한 것으로 표시됨	모니터링된 인터페이스 또는 페일오버 링크에 대한 hello 메시지가 수신되지 않음

오류 이벤트	정책	액티브 유닛 조치	스탠바이 유닛 조치	참고
이전 액티브 유닛 복구	페일오버 없음	스탠바이 상태가 됨	작업 없음	없음
스탠바이 유닛 오류(전력 또는 하드웨어)	페일오버 없음	스탠바이가 실패한 것으로 표시됨	해당 없음	스탠바이 유닛이 실패한 것으로 표시될 경우, 액티브 유닛에서는 페일오버를 시도하지 않으며 인터페이스 오류 임계값을 넘은 경우에도 마찬가지입니다.
작동 중 페일오버 링크에 오류 발생	페일오버 없음	페일오버 링크가 실패한 것으로 표시됨	페일오버 링크가 실패한 것으로 표시됨	페일오버가 중단된 동안에는 유닛에서 스탠바이 유닛으로 페일오버를 시작하지 못하므로 최대한 빨리 페일오버 링크를 복구해야 합니다.
시작 시 페일오버 링크에 오류 발생	페일오버 없음	액티브 상태가 됨 페일오버 링크가 실패한 것으로 표시됨	액티브 상태가 됨 페일오버 링크가 실패한 것으로 표시됨	시작 시 페일오버 링크가 중단되면 두 유닛 모두 액티브 상태가 됩니다.
상태 링크 오류 발생	페일오버 없음	작업 없음	작업 없음	페일오버가 실행될 경우 상태 정보가 최신이 아닌 것으로 변경되며 세션이 종료됩니다.
임계값을 넘은 액티브 유닛에서 인터페이스 오류 발생	페일오버	액티브가 실패한 것으로 표시됨	액티브 상태가 됨	없음
임계값을 넘은 스탠바이 유닛에서 인터페이스 오류 발생	페일오버 없음	작업 없음	스탠바이가 실패한 것으로 표시됨	스탠바이 유닛이 실패한 것으로 표시될 경우, 액티브 유닛에서는 페일오버를 시도하지 않으며 인터페이스 오류 임계값을 넘은 경우에도 마찬가지입니다.

페일오버 및 스테이트풀 페일오버 링크

페일오버 링크는 두 유닛 사이의 전용 연결입니다. 스테이트풀 페일오버 링크 역시 전용 연결이지만, 페일오버 링크 하나를 페일오버/상태가 결합된 링크로 사용할 수도 있고 별도의 전용 상태 링크를 생

성할 수도 있습니다. 페일오버 링크만 사용하는 경우에는 스테이트풀 정보가 해당 링크를 통해 전송되며 스테이트풀 페일오버 기능도 유지됩니다.

기본적으로 페일오버 및 스테이트풀 페일오버 링크의 통신은 암호화되지 않은 일반 텍스트로 이루어집니다. IPsec 암호화 키를 구성하면 통신을 암호화하여 보안을 강화할 수 있습니다.

다음 주제에서는 이러한 인터페이스에 대해 더 자세히 설명하며, 최고의 결과를 얻기 위해 디바이스를 유선 연결하는 방법에 대한 권장 사항을 제공합니다.

페일오버 링크

페일오버 쌍의 두 유닛은 페일오버 링크를 통해 지속적으로 통신하여 각 유닛의 작동 상태를 확인하고 컨피그레이션 변경 사항을 동기화합니다.

다음 정보는 페일오버 링크를 통해 전달됩니다.

- 유닛 상태(액티브 또는 스탠바이).
- Hello 메시지(keep-alive).
- 네트워크 링크 상태.
- MAC 주소 교환.
- 컨피그레이션 복제 및 동기화.
- 시스템 데이터베이스 업데이트. 여기에는 VDB 및 규칙은 포함되지만 지리위치 및 보안 인텔리전스 데이터베이스는 포함되지 않습니다. 각 시스템은 지리위치 및 보안 인텔리전스 업데이트를 개별적으로 다운로드합니다. 업데이트 일정을 생성하는 경우에는 동기화 상태를 유지해야 합니다. 하지만 액티브 디바이스에서 수동 지리위치 또는 보안 인텔리전스 업데이트를 수행하는 경우에는 스탠바이 디바이스에서도 업데이트를 수행해야 합니다.



참고 이벤트, 보고 및 감사 로그 데이터는 동기화되지 않습니다. 이벤트 뷰어 및 대시보드에는 지정된 유닛과 관련된 데이터만 표시됩니다. 또한 구축 기록, 작업 기록 및 기타 감사 로그 이벤트는 동기화되지 않습니다.

스테이트풀 페일오버 링크

시스템은 상태 링크를 사용해 연결 상태 정보를 스탠바이 디바이스에 전달합니다. 페일오버 수행 시에 스탠바이 유닛은 이 정보를 사용하여 기존 연결을 유지할 수 있습니다.

인터페이스를 유지하는 가장 좋은 방법은 페일오버 및 스테이트풀 페일오버 링크 모두에 단일 링크를 사용하는 것입니다. 그러나 컨피그레이션 규모가 크고 네트워크의 트래픽이 많은 경우에는 상태 링크와 페일오버 링크에 대해 전용 인터페이스를 사용하는 것을 고려해야 합니다.

장애 조치 및 상태 링크의 인터페이스

사용되지 않지만 활성화되어 있는 데이터 인터페이스(물리적 또는 EtherChannel)를 장애 조치 링크로 사용할 수 있습니다. 그러나 현재 이름이 구성된 인터페이스는 지정할 수 없습니다. 장애 조치 링크

인터페이스는 일반적인 네트워킹 인터페이스로 구성되지 않으며, 장애 조치 통신용으로만 존재합니다. 이 인터페이스는 장애 조치 링크용으로만 사용할 수 있습니다(또한 상태 링크용으로도 사용 가능). 장애 조치에는 관리 인터페이스, 하위 인터페이스, VLAN 인터페이스 또는 스위치 포트를 사용할 수 없습니다.

threat defense 디바이스에서는 사용자 데이터와 장애 조치 링크 간에 인터페이스 공유를 지원하지 않습니다.

장애 조치 및 상태 링크 크기 조정에 대한 다음 지침을 참조하십시오.

- Firepower 4100/9300 - 페일오버 및 상태 링크를 통합하려면 10GB 데이터 인터페이스를 사용하는 것이 좋습니다.
- 기타 모델 - 1GB 인터페이스는 통합된 장애 조치 및 상태 링크에 충분한 크기입니다.

EtherChannel 인터페이스를 장애 조치 또는 상태 링크로 사용하는 경우,고가용성을 설정하기 전에 동일한 ID 및 멤버 인터페이스를 사용하는 동일한 EtherChannel이 두 디바이스에 있는지 확인해야 합니다. EtherChannel이 일치하지 않는 경우에는 HA를 비활성화하고 이전의 보조 유닛에서 구성을 수정해야 합니다. 패킷의 오류를 방지하기 위해 EtherChannel에서는 하나의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다. 장애 조치 링크로 사용 중인 경우 EtherChannel 컨피그레이션을 변경할 수 없습니다.

페일오버 및 스테이트풀 페일오버 인터페이스 연결

사용되지 않는 모든 데이터 물리적 인터페이스를 페일오버 링크 및 전용 상태 링크(선택 사항)로 사용할 수 있습니다. 그러나 현재 특정 이름으로 구성되어 있거나 하위 인터페이스가 있는 인터페이스는 선택할 수 없습니다. 페일오버 및 스테이트풀 페일오버 링크 인터페이스는 일반 네트워킹 인터페이스로 구성되지 않습니다. 이러한 인터페이스는 페일오버 통신에만 사용되며 통과 트래픽 또는 관리 액세스에는 사용할 수 없습니다.

컨피그레이션이 디바이스 간에 동기화되므로 링크의 양쪽 끝에 같은 포트 번호를 선택해야 합니다. 예를 들어 페일오버 링크를 위해 두 디바이스에서 모두 GigabitEthernet1/3을 선택합니다.

다음의 두 가지 방식 중 하나로 페일오버 링크와 전용 상태 링크(사용하는 경우)를 연결합니다.

- 같은 네트워크 세그먼트(브로드캐스트 도메인 또는 VLAN)에 다른 디바이스가 없는 상태에서 스위치를 threat defense 디바이스의 페일오버 인터페이스로 사용합니다. 전용 상태 링크의 요구 사항도 같지만, 이 링크는 페일오버 링크와 다른 네트워크 세그먼트에 있어야 합니다.



참고 스위치를 사용하는 장점은 유닛 인터페이스 중 하나가 중단되는 경우 장애가 발생한 인터페이스를 쉽게 트러블슈팅할 수 있다는 것입니다. 다이렉트 케이블 연결을 사용하는 경우 인터페이스 하나에서 장애가 발생하면 두 피어에서 모두 링크가 중단되므로 결함이 있는 디바이스를 확인하기가 어렵습니다.

- 외부 스위치를 사용할 필요 없이 이더넷 케이블을 사용하여 유닛을 직접 연결합니다. threat defense에서는 구리 이더넷 포트의 Auto-MDI/MDIX를 지원하므로 crossover 케이블 또는 straight-through

케이블을 사용할 수 있습니다. 다이렉트 케이블을 사용할 경우 인터페이스에서는 케이블을 자동으로 감지하고 송/수신 쌍 중 하나를 MDIX로 교체합니다.

장거리 페일오버를 사용할 경우 최적의 성능을 보장하려면 페일오버 링크의 레이턴시는 10밀리초 미만이어야 하고 250밀리초를 초과해서는 안 됩니다. 레이턴시가 10밀리초를 초과하는 경우 페일오버 메시지의 재전송으로 인해 성능이 다소 저하됩니다.

페일오버 및 데이터 링크 중단 방지

페일오버 링크 및 데이터 인터페이스가 다른 경로를 통해 이동하도록 설정하여 모든 인터페이스에 동시 다발적으로 오류가 발생하는 가능성을 줄이는 것이 좋습니다. 페일오버 링크가 중단될 경우 threat defense 디바이스는 데이터 인터페이스를 사용하여 페일오버가 필요한지 여부를 확인할 수 있습니다. 그런 다음 페일오버 링크 상태가 복원될 때까지는 페일오버 작업이 보류됩니다.

복원력이 뛰어난 페일오버 네트워크를 설계하려면 다음 연결 시나리오를 참조하십시오.

시나리오 1 — 권장하지 않음

단일 스위치 또는 스위치 집합을 사용하여 두 threat defense 디바이스 간의 페일오버 및 데이터 인터페이스를 모두 연결한 상태에서 스위치 또는 스위치 간 링크가 중단될 경우 두 threat defense 디바이스 모두 액티브 상태가 됩니다. 따라서 아래의 그림에 있는 다음 2가지 연결 방법은 권장하지 않습니다.

그림 1: 단일 스위치로 연결 - 권장하지 않음

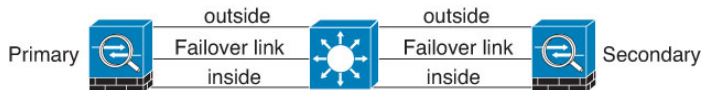
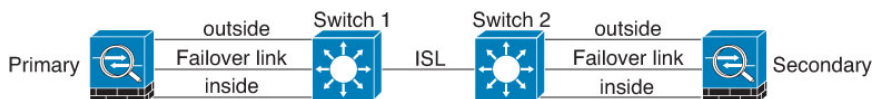


그림 2: 이중 스위치로 연결 - 권장하지 않음



시나리오 2 - 권장함

페일오버 링크에서는 데이터 인터페이스와 같은 스위치를 사용하지 않는 것이 좋습니다. 대신 다음 그림에 나와 있는 것처럼 다른 스위치를 사용하거나 다이렉트 케이블을 사용하여 페일오버 링크에 연결합니다.

그림 3: 다른 스위치로 연결

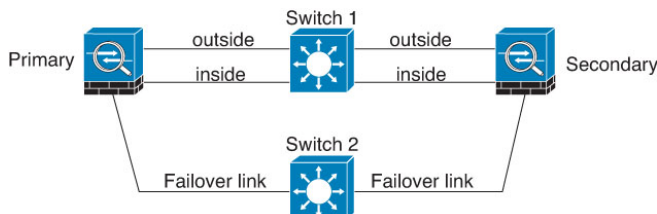
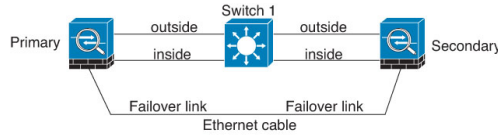


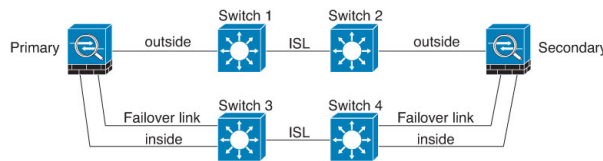
그림 4: 케이블로 연결



시나리오 3 — 권장

threat defense 데이터 인터페이스가 여러 개의 스위치 집합에 연결되어 있는 경우, 페일오버 링크는 이러한 스위치 중 하나에 연결될 수 있으며 다음 그림에 나온 것처럼 주로 네트워크의 보안(내부) 측에 있는 스위치일 가능성이 높습니다.

그림 5: 보안 스위치로 연결



스테이트풀 페일오버가 사용자 연결에 주는 영향

액티브 유닛은 스탠바이 유닛과 연결 상태 정보를 공유합니다. 즉, 스탠바이 유닛은 사용자에게 영향을 주지 않고 특정 유형의 연결을 유지할 수 있습니다.

그러나 스테이트풀 페일오버를 지원하지 않는 연결 유형도 있습니다. 이러한 연결의 경우, 페일오버가 있으면 사용자가 연결을 다시 설정해야 합니다. 이러한 과정은 대개 연결에 사용되는 프로토콜의 동작을 기반으로 하여 자동으로 진행되는 경우가 많습니다.

다음 주제에서는 스테이트풀 페일오버에 지원되는 기능과 지원되지 않는 기능을 설명합니다.

지원 기능

스테이트풀 페일오버에서는 다음 상태 정보가 스탠바이 위협 방지 디바이스로 전달됩니다.

- NAT 변환 테이블.
- TCP 및 UDP 연결과 상태(HTTP 연결 상태 포함). 다른 유형의 IP 프로토콜과 ICMP는 새 패킷이 도착하면 새 액티브 유닛에서 설정되므로 액티브 유닛에서 구문 분석되지 않습니다.
- Snort 연결 상태, 검사 결과 및 핀홀 정보(엄격한 TCP 적용 포함).
- ARP 테이블
- 레이어 2 브리지 테이블(브리지 그룹용)
- ISAKMP 및 IPsec SA 테이블
- GTP PDP 연결 데이터베이스
- SIP 시그널링 세션 및 핀홀.

- 정적 및 동적 라우팅 테이블 - 스테이트풀 페일오버는 OSPF 및 EIGRP 같은 동적 라우팅 프로토콜에 참여하므로, 액티브 유닛에서 동적 라우팅 프로토콜을 통해 확인한 경로는 스텐바이 유닛의 RIB(Routing Information Base) 테이블에 유지됩니다. 페일오버 이벤트 발생 시 액티브 보조 유닛에서는 초기 규칙에 따라 기본 유닛을 미러링하므로 트래픽 중단을 최소화하면서도 패킷이 정상적으로 이동됩니다. 페일오버가 끝난 직후에는 새 액티브 유닛에서 재통합 타이머가 시작됩니다. 그러면 RIB 테이블의 시간대 숫자가 늘어납니다. 재통합을 수행하는 동안 OSPF 및 EIGRP 경로는 새 시간대 숫자로 업데이트됩니다. 타이머가 만료되면 오래된 경로 항목(시간대 숫자에 의해 결정됨)이 테이블에서 제거됩니다. 그런 다음 RIB에 새 액티브 유닛에 대한 최신 라우팅 프로토콜 전달 정보가 포함됩니다.



참고 경로는 액티브 유닛의 링크 작동 또는 링크 중단 이벤트가 있을 경우에만 동기화됩니다. 스텐바이 유닛에서 링크가 작동하거나 중단될 경우, 액티브 유닛에서 전송된 동적 경로가 손실될 수 있습니다. 이는 일반적인 동작입니다.

- DHCP 서버 - DHCP 주소 임대는 복제되지 않습니다. 그러나 인터페이스에 구성된 DHCP 서버는 ping을 전송하여 특정 주소가 사용 중이지 않음을 확인한 후에 DHCP 클라이언트에 해당 주소를 부여하므로 서비스에는 영향이 없습니다. 상태 정보는 DHCP 릴레이 또는 DDNS와 관련이 없습니다.
- 액세스 제어 정책 결정 - 트래픽 일치(URL, URL 카테고리, 지리위치 등), 침입 탐지, 악성코드 및 파일 유형과 관련된 결정은 페일오버 중에 그대로 유지됩니다. 그러나 페일오버 시점에서 평가 중인 연결의 경우 다음 경고가 적용됩니다.
 - AVC - 앱-ID 판정은 복제되지만 탐지 상태는 복제되지 않습니다. 페일오버가 수행되기 전에 앱-ID 판정이 완료 및 동기화되면 적절한 동기화가 수행됩니다.
 - 침입 탐지 상태 - 페일오버 시 중간 플로우 픽업이 발생하면 새 검사는 완료되지만 이전 상태는 손실됩니다.
 - 파일 악성코드 차단 - 페일오버 전에 파일 상태를 확인할 수 있어야 합니다.
 - 파일 유형 탐지 및 차단 - 페일오버 전에 파일 유형이 식별되어야 합니다. 원래 액티브 디바이스가 파일을 식별하는 중에 페일오버가 수행되면 파일 유형이 동기화되지 않습니다. 따라서 파일 정책에서 해당 파일 유형을 차단하더라도 새 액티브 디바이스는 파일을 다운로드합니다.
- ID 정책의 패시브 사용자 ID 결정(종속 포털을 통한 활성 인증을 통해 수집된 결정은 제외).
- 보안 인텔리전스 결정.
- RA VPN - 원격 액세스 VPN 최종 사용자는 페일오버 후 VPN 세션을 다시 인증하거나 다시 연결하지 않아도 됩니다. 그러나 VPN 연결을 통해 작동하는 애플리케이션의 경우 페일오버 프로세스 도중 패킷이 손실될 수 있으며 패킷이 손실되면 복구되지 않습니다.
- 모든 연결 중에서 설정된 연결만 스텐바이 ASA에 복제됩니다.

지원되지 않는 기능

스태이트풀 페일오버에서는 다음 상태 정보가 스탠바이 위협 방지 디바이스로 전달되지 않습니다.

- GRE 또는 IP-in-IP와 같은 일반 텍스트 터널의 . 터널 내의 세션은 복제되지 않으며, 새 액티브 노드는 기존 검사 관정을 재사용하여 정확한 정책 규칙 일치 여부를 확인할 수 없습니다.
- 암호 해독된 TLS/SSL 연결 - 암호 해독 상태가 동기화되지 않고 만약 액티브 유닛에 장애가 발생하면 암호 해독된 연결이 재설정됩니다. 새 활성 유닛에 새 연결을 설정해야 합니다. 암호 해독되지 않은 연결(TLS/SSL 암호 해독 안 함 규칙 작업과 일치하는 연결)은 영향을 받지 않으며, 올바르게 복제됩니다.
- 멀티캐스트 라우팅.

스탠바이 유닛에서 허용되는 컨피그레이션 변경 사항 및 작업

고가용성 모드에서 작동 중일 때는 액티브 유닛에서만 컨피그레이션을 변경합니다. 컨피그레이션을 구축하면 새 변경 사항이 스탠바이 유닛에도 전송됩니다.

하지만 스탠바이 유닛에만 있는 속성도 있습니다. 스탠바이 유닛에서 변경할 수 있는 항목은 다음과 같습니다.

- 관리 IP 주소 및 게이트웨이.
- (CLI에서만 가능) 관리자 사용자 계정 및 기타 로컬 사용자 계정의 비밀번호. CLI에서만 이것을 변경할 수 있고, device manager에서는 할 수 없습니다. 모든 로컬 사용자는 두 유닛 모두의 비밀번호를 개별적으로 변경해야 합니다.

또한 스탠바이 디바이스에서는 다음과 같은 작업이 가능합니다.

- 고가용성 작업(예: HA 일시 중단, 다시 시작, 재설정, 해제, 액티브 및 스탠바이 유닛 간 모드 전환).
- 대시보드 및 이벤트 데이터는 디바이스별로 고유하며 동기화되지 않습니다. 여기에는 이벤트 뷰어의 맞춤형 보기가 포함됩니다.
- 감사 로그 정보는 디바이스별로 고유합니다.
- 스마트 라이선싱 등록. 그러나 선택적 라이선스는 액티브 유닛에서 활성화하거나 비활성화해야 하며, 해당 작업은 스탠바이 유닛과 동기화됩니다. 그러면 스탠바이 유닛이 적절한 라이선스를 요청하거나 해제합니다.
- 백업(복원은 아님). 백업을 복원하려면 유닛에서 HA를 해제해야 합니다. 백업이 HA 컨피그레이션을 포함하는 경우 유닛이 HA 그룹에 다시 조인합니다.
- 소프트웨어 업그레이드 설치.
- 트러블슈팅 로그 생성.

- 지리위치 또는 보안 인텔리전스 데이터베이스 수동 업데이트. 이러한 데이터베이스는 유닛 간에 동기화되지 않습니다. 업데이트 일정을 생성하는 경우 유닛은 일관성을 독립적으로 유지할 수 있습니다.
- **Monitoring(모니터링) > Sessions(세션)** 페이지에서 활성 **device manager** 사용자 세션을 볼 수 있으며 세션을 삭제할 수 있습니다.

고가용성을 위한 시스템 요구 사항

다음 주제에서는 고가용성 컨피그레이션으로 두 디바이스를 통합하기 전에 충족해야 하는 요구 사항을 설명합니다.

HA의 하드웨어 요구 사항

고가용성 컨피그레이션에서 두 디바이스를 연결하려면 다음 하드웨어 요구 사항을 충족해야 합니다.

- 디바이스의 하드웨어 모델이 정확히 동일해야 합니다.
Firepower 9300의 경우 고가용성은 동일한 유형의 모듈 간에만 지원되지만, 두 새시는 혼합된 모듈을 포함할 수 있습니다. 예를 들어, 각 새시에는 SM-36 및 SM-44가 있습니다. SM-36 모듈 간, SM-44 모듈 간에 고가용성 쌍을 생성할 수 있습니다.
- 디바이스의 인터페이스 수와 유형이 동일해야 합니다.
Firepower 4100/9300 새시의 경우, HA를 활성화하기 전에 FXOS에서 모든 인터페이스를 사전에 동일하게 구성해야 합니다. HA를 활성화한 후에 인터페이스를 변경하는 경우에는 스탠바이 유닛의 FXOS에서 인터페이스를 변경한 다음, 액티브 유닛에서 동일하게 변경을 수행합니다.
- 디바이스에 동일한 모듈이 설치되어 있어야 합니다. 예를 들어, 한 디바이스에 네트워크 인터페이스 모듈(선택 사항)이 있는 경우 다른 디바이스에도 동일한 모듈을 설치해야 합니다.
- Firepower 9300용 새시 내 고가용성은 지원되지 않습니다. 동일한 Firepower 9300새시에서 별도의 논리적 디바이스 간에 HA를 구성할 수는 없습니다.

HA의 소프트웨어 요구 사항

고가용성 컨피그레이션에서 두 디바이스를 연결하려면 다음 소프트웨어 요구 사항을 충족해야 합니다.

- 두 디바이스가 정확히 동일한 소프트웨어 버전을 실행해야 합니다. 즉, 주 버전 번호(첫 번째), 부 버전 번호(두 번째) 및 유지 보수 버전 번호(세 번째)가 같아야 합니다. **device manager**의 **Devices(디바이스)** 페이지에서 버전을 확인하거나 CLI에서 **show version** 명령을 사용할 수 있습니다. 각기 다른 버전이 설치된 디바이스도 조인할 수는 있지만, 유닛을 같은 소프트웨어 버전으로 업그레이드할 때까지는 컨피그레이션을 스탠바이 유닛으로 가져올 수 없으며 페일오버가 작동하지 않습니다.

- 두 디바이스가 모두 로컬 관리자 모드여야 합니다(device manager을 사용하여 구성되어 있어야 함). 두 시스템에서 모두 device manager에 로그인할 수 있다면 로컬 관리자 모드인 것입니다. CLI에서 **show managers** 명령을 사용하여 확인할 수도 있습니다.
- 각 디바이스에 대해 초기 설정 마법사를 완료해야 합니다.
- 각 디바이스에 자체 관리 IP 주소가 있어야 합니다. 관리 인터페이스의 컨피그레이션은 디바이스 간에 동기화되지 않습니다.
- 디바이스의 NTP 컨피그레이션이 같아야 합니다.
- DHCP를 사용하여 주소를 획득하도록 인터페이스를 구성할 수는 없습니다. 즉, 모든 인터페이스에 고정 IP 주소가 있어야 합니다.
- 클라우드 서비스의 경우 두 디바이스를 같은 지역에 등록해야 하거나 두 디바이스를 모두 등록할 수 없습니다. 혼합 클라우드 서비스 등록은 할 수 없습니다.
- 고가용성을 구성하기 전에 보류 중인 변경 사항을 모두 구축해야 합니다.

HA의 라이선스 요구 사항

유닛은 고가용성을 구성하기 전에 동일한 상태여야 합니다. 즉, 두 유닛이 모두 Base 라이선스로 등록되어 있거나 평가 모드여야 합니다. 등록된 디바이스는 다른 Cisco Smart Software Manager 어카운트에 등록할 수 있습니다. 단, 이러한 어카운트의 내보내기 제어 기능 설정 상태가 같아야 합니다(둘 다 활성화되어 있거나 비활성화되어 있어야 함). 그러나 각 유닛에 각기 다른 선택적 라이선스를 활성화했는지는 중요하지 않습니다. 두 유닛을 모두 등록하는 경우, 디바이스에 대해 동일한 Cisco Cloud Services 지역을 선택해야 합니다.

디바이스가 등록된 경우 스마트 라이선스 또는 PLR(영구 라이선스 예약) 중 하나의 모드를 동일하게 사용해야 합니다.

작동 중에는 고가용성 쌍의 유닛은 라이선스가 동일해야 합니다. 활성 유닛에서의 라이선스 변경은 구축 중에 스탠바이 유닛에서도 반복됩니다.

고가용성 컨피그레이션에서는 디바이스 쌍의 각 디바이스에 대해 하나씩, 두 개의 Smart License 자격이 필요합니다. 어카운트에 각 디바이스에 적용할 라이선스가 충분한지 확인해야 합니다. 라이선스가 부족하면 디바이스별로 컴플라이언스 상태가 달라질 수 있습니다.

예를 들어 액티브 디바이스에는 Base 라이선스와 위협 라이선스가 있는데 스탠바이 디바이스에 Base 라이선스만 있는 경우, 스탠바이 유닛은 Cisco Smart Software Manager와 통신하여 어카운트에서 사용할 가능한 위협 라이선스를 가져옵니다. Smart License 어카운트에 구매한 자격이 충분히 없으면, 정확한 수의 라이선스를 구매할 때까지 어카운트는 컴플라이언스 위반 상태가 됩니다(액티브 디바이스는 컴플라이언스 준수 상태이더라도 스탠바이 디바이스는 컴플라이언스 위반 상태).



참고 내보내기 제어 기능에 대한 설정이 서로 다른 계정에 디바이스를 등록하거나 한 유닛은 등록하고 다른 유닛은 평가 모드에 있는 HA 쌍을 생성하려는 경우, HA 가입에 실패할 수 있습니다. 내보내기 제어 기능에 대한 일관성 없는 설정으로 IPsec 암호화 키를 구성하면 HA를 활성화한 후에 두 디바이스가 모두 활성화됩니다. 이로 인해 지원되는 네트워크 세그먼트에서의 라우팅이 영향을 받게 되고, 이를 복구하기 위해서는 보조 유닛에서 HA를 수동으로 해제해야 합니다.

고가용성에 대한 지침

모델 지원

- Firepower 9300 - Firepower 9300에서 HA를 구성할 수 있습니다. 그러나 동일한 Firepower 9300 새 시에서 별도의 논리적 디바이스 간에 HA를 컨피그레이션할 수는 없습니다.
- Firepower 1010:
 - 고가용성 사용 시 스위치 포트 기능을 사용해서는 안 됩니다. 스위치 포트는 하드웨어에서 작동하므로 액티브 및 스탠바이 유닛에서 계속 트래픽을 전달합니다. 고가용성은 트래픽이 스탠바이 유닛을 통과하는 것을 방지하기 위해 고안되었지만 스위치 포트로 확장되지는 않습니다. 일반 고가용성 네트워크 설정에서 두 유닛의 액티브 스위치 포트는 네트워크 루프로 이어집니다. 모든 스위칭 기능에는 외부 스위치를 사용하는 것이 좋습니다. VLAN 인터페이스는 장애 조치를 통해 모니터링될 수 있지만 스위치 포트는 그럴 수 없습니다. 이론적으로는 VLAN에 단일 스위치 포트를 배치하고 고가용성을 정상적으로 사용할 수 있지만, 물리적 방화벽 인터페이스를 대신 사용하면 더 간단하게 설정할 수 있습니다.
 - 방화벽 인터페이스만 장애 조치 링크로 사용할 수 있습니다.
- Threat Defense Virtual — HA 컨피그레이션은 Microsoft Azure Cloud 또는 AWS(Amazon Web Services) Cloud용 threat defense virtual에 대해 지원되지 않습니다.

추가 지침

- 169.254.0.0/16 및 fd00:0:0::*:/64는 내부적으로 사용되는 서브넷이며 페일오버 또는 상태 링크에 사용할 수 없습니다.
- 액티브 유닛에서 컨피그레이션 작업을 실행하면 액티브 유닛에서 구축 작업을 실행할 때 스탠바이 유닛에 동기화됩니다. 그러나 일부 변경 사항은 스탠바이 유닛에 동기화되지 않은 상태라 하더라도 해당 변경 사항을 구축할 때까지는 보류 중 변경 사항에 표시되지 않습니다. 다음 중 어느 것을 변경하는 경우, 해당 변경 사항은 표시되지 않으며 먼저 구축 작업을 실행해야 스탠바이 유닛에 컨피그레이션됩니다. 변경 사항을 즉시 적용해야 하는 경우, 보류 중인 변경 사항에 표시되는 다른 변경 작업을 수행해야 합니다. 표시되지 않은 변경 사항에는 규칙 예약, 지오데이터베이스, 보안 인텔리전스 또는 VDB 업데이트, 백업 예약, NTP, 관리 인터페이스용 DNS, 등에 대한 수정 사항이 포함되어 있습니다.

- 기본 유닛과 보조 유닛에서 모두 백업을 수행해야 합니다. 백업을 복원하려면 먼저 HA를 해제해야 합니다. 두 유닛에서 동일한 백업을 복원하지 마십시오. 이렇게 하면 두 유닛이 모두 액티브로 설정됩니다. 대신 액티브로 설정할 유닛에서 백업을 먼저 복원한 후에 다른 유닛에서 해당하는 백업을 복원합니다.
- 여러 ID 소스의 **Test(테스트)** 버튼은 액티브 유닛에서만 작동합니다. 스탠바이 디바이스에 대한 ID 소스 연결을 테스트해야 하는 경우 먼저 모드를 전환하여 스탠바이 피어를 액티브 피어로 설정해야 합니다.
- 고가용성 컨피그레이션을 생성하거나 해제하는 경우, 컨피그레이션 변경 사항을 구축하면 두 디바이스에서 모두 Snort 검사 프로세스가 재시작됩니다. 그러면 프로세스가 완전히 재시작될 때까지 통과 트래픽이 중단될 수 있습니다.
- 고가용성을 처음 구성할 때 보조 유닛의 보안 인텔리전스 및 지리위치 데이터베이스 버전이 기본 유닛과 다르면 데이터베이스를 업데이트하는 작업이 보조 유닛에서 예약됩니다. 이러한 작업은 액티브 유닛에서 다음 구축 시에 실행됩니다. HA 조인에 실패하는 경우 이러한 작업은 유지되며 다음 구축 시에 실행됩니다.
- 액티브 유닛에서 스탠바이 유닛으로 페일오버를 시작할 경우, STP(Spanning Tree Protocol)를 실행 중인 연결된 스위치 포트에서는 토폴로지 변경을 인지하는 경우 30초 ~ 50초 동안 차단 상태가 될 수 있습니다. 포트가 차단 상태일 때 트래픽 손실을 방지하기 위해 스위치에서 STP PortFast 기능을 활성화할 수 있습니다.

interface interface_id spanning-tree portfast

이 해결 방법은 라우팅 모드 및 브리지 그룹 인터페이스에 모두 연결된 스위치에 적용됩니다. PortFast 기능을 사용하면 링크 작동 시 포트가 STP 전달 모드로 즉시 전환됩니다. 포트는 STP에 계속 참여합니다. 따라서 포트가 루프의 일부인 경우 포트가 STP 차단 모드로 전환됩니다.

- 고가용성 쌍에 연결된 스위치에서 포트 보안을 구성할 경우 페일오버 이벤트가 발생할 때 통신에 문제가 생길 수 있습니다. 이러한 문제는 한 보안 포트에서 구성하거나 확인한 보안 MAC 주소가 다른 보안 포트에 이동될 경우 발생하며, 스위치 포트 보안 기능에 의해 위반 여부가 플래그로 표시됩니다.
- 액티브/스탠바이 고가용성 및 VPN IPsec 터널의 경우, VPN 터널을 통해 SNMP를 사용하여 액티브 유닛과 스탠바이 유닛을 모두 모니터링할 수는 없습니다. 스탠바이 유닛에는 활성화 VPN 터널이 없으며 NMS(Network Management System)로 전송되는 트래픽은 삭제됩니다. 암호화 기능이 있는 SNMPv3을 대신 사용하면 IPsec 터널을 사용하지 않아도 됩니다.

고가용성 구성

디바이스에서 장애가 발생하더라도 네트워크에 연결할 수 있도록 하려면 고가용성 설정을 사용합니다. 액티브/스탠바이 고가용성을 사용하는 경우에는 두 디바이스가 연결되므로 액티브 디바이스에서 장애가 발생하면 스탠바이 디바이스가 작업을 이어받으며 사용자에는 연결 문제가 잠시 동안만 표시됩니다.

다음 절차에서는 액티브/스탠바이 고가용성 쌍을 설정하는 전체 프로세스를 설명합니다.

프로시저

- 단계 1 [고가용성을 위한 두 유닛 준비, 14 페이지.](#)
- 단계 2 [고가용성을 위한 기본 유닛 구성, 16 페이지.](#)
- 단계 3 [고가용성을 위한 보조 유닛 구성, 19 페이지.](#)
- 단계 4 [상태 모니터링을 위한 페일오버 기준 구성, 20 페이지.](#)

기준에는 피어 모니터링과 인터페이스 모니터링이 포함됩니다. 모든 페일오버 기준에는 기본 설정이 있지만, 최소한 기본 설정을 검사하여 네트워크에서 기본 설정이 작동하는지를 확인해야 합니다.

- [피어 유닛 상태 모니터링 페일오버 기준 구성, 21 페이지.](#)
- [인터페이스 상태 모니터링 페일오버 기준 구성, 22 페이지.](#)

인터페이스 테스트에 대한 정보는 [시스템이 인터페이스 상태를 테스트하는 방법, 24 페이지](#)의 내용을 참조하십시오.

- 단계 5 (선택 사항, 권장함.) [스탠바이 IP 및 MAC 주소 구성, 25 페이지.](#)
- 단계 6 (선택 사항.) [고가용성 컨피그레이션 확인, 26 페이지.](#)

고가용성을 위한 두 유닛 준비

고가용성을 적절하게 구성하려면 몇 가지 사항을 정확하게 준비해야 합니다.

프로시저

- 단계 1 디바이스가 [HA의 하드웨어 요구 사항, 10 페이지](#)에 설명되어 있는 요구 사항을 충족하는지 확인합니다.
- 단계 2 단일 페일오버 링크를 사용할 것인지 아니면 별도의 페일오버 링크와 스테이트풀 페일오버 링크를 사용할지를 결정하고, 사용할 포트를 식별합니다.

각 링크에 대해 각 디바이스에서 같은 포트 번호를 사용해야 합니다. 예를 들어 두 디바이스에서 모두 페일오버 링크용으로 GigabitEthernet 1/3을 사용합니다. 실수로 해당 포트 번호를 다른 용도에 사용하는 일이 없도록, 사용할 포트를 확실히 파악해야 합니다. 자세한 내용은 [페일오버 및 스테이트풀 페일오버 링크, 3 페이지](#)를 참고하십시오.
- 단계 3 디바이스를 설치하고 네트워크에 연결한 다음 각 디바이스에서 초기 설정 마법사를 완료합니다.
 - a) [페일오버 및 데이터 링크 중단 방지, 6 페이지](#)에서 권장 네트워크 설계를 검토합니다.
 - b) [인터페이스 연결](#)에 설명된 대로 최소한 외부 인터페이스를 연결합니다.

다른 인터페이스도 연결할 수 있지만, 이 경우에는 각 디바이스에서 동일한 포트를 사용하여 지정된 서브넷에 연결해야 합니다. 디바이스는 같은 컨피그레이션을 공유하므로 병렬 방식으로 네트워크에 연결해야 합니다.

참고 설정 마법사에서는 관리 및 내부 인터페이스의 IP 주소를 변경할 수 없습니다. 그러므로 기본 디바이스에서 이러한 인터페이스 중 하나를 네트워크에 연결하는 경우 보조 디바이스에서도 해당 인터페이스를 연결하면 안 됩니다. 이렇게 하면 IP 주소가 충돌하게 됩니다. 워크스테이션을 이러한 인터페이스 중 하나에 직접 연결하고 DHCP를 통해 주소를 얻을 수 있습니다. 그러면 **device manager**에 연결하여 디바이스를 구성할 수 있습니다.

- c) 각 디바이스에서 초기 설정 마법사를 완료합니다. 외부 인터페이스에 대한 정적 IP 주소를 지정했는지 확인합니다. 그리고 동일한 NTP 서버를 구성합니다. 자세한 내용은 [설정 마법사를 사용하여 초기 컨피그레이션 완료](#)를 참고하십시오.

유닛에 대해 동일한 라이선싱 및 Cisco Success Network 옵션을 선택합니다. 예를 들어 각 유닛을 평가 모드로 설정하거나 디바이스를 등록합니다.

- d) 보조 디바이스에서 **Device(디바이스) > System Settings(시스템 설정) > Management Interface(관리 인터페이스)**를 선택한 다음 고유한 IP 주소를 구성하고, 필요한 경우 게이트웨이를 변경하고, 필요에 맞게 DHCP 서버 설정을 비활성화하거나 변경합니다.
- e) 보조 디바이스에서 **Device(디바이스) > Interface(인터페이스)**를 선택하고 내부 인터페이스를 수정합니다. IP 주소를 삭제하거나 변경합니다. 또한 인터페이스에 대해 정의된 DHCP 서버를 삭제합니다. 같은 네트워크에 DHCP 서버가 두 개일 수는 없기 때문입니다.
- f) 보조 디바이스에서 컨피그레이션을 구축합니다.
- g) 네트워크 토폴로지에 따라 필요한 경우 기본 디바이스에 로그인한 다음 관리 주소, 게이트웨이 및 DHCP 서버 설정과 내부 인터페이스 IP 주소 및 DHCP 서버 설정을 변경합니다. 변경을 하는 경우에는 컨피그레이션을 구축합니다.
- h) 내부 인터페이스 또는 관리 인터페이스(별도의 관리 네트워크 사용 시)를 연결하지 않은 경우에는 지금 해당 인터페이스를 스위치에 연결할 수 있습니다.

단계 4 디바이스의 소프트웨어 버전이 정확히 동일한지 확인합니다. 주 버전 번호(첫 번째 숫자), 부 버전 번호(두 번째 숫자) 및 유지 보수 버전 번호(세 번째 숫자)가 같아야 합니다. **device manager**의 **Devices(디바이스)** 페이지에서 버전을 확인하거나 CLI에서 **show version** 명령을 사용할 수 있습니다.

디바이스가 동일한 소프트웨어 버전을 실행하고 있지 않다면 [Cisco.com](#)에서 원하는 소프트웨어 버전을 다운로드하여 각 디바이스에 설치합니다. 자세한 내용은 [Threat Defense 소프트웨어 업그레이드](#)를 참조해 주십시오.

단계 5 페일오버 및 스테이트풀 페일오버 링크를 연결하고 구성합니다.

- a) [페일오버 및 데이터 링크 중단 방지, 6 페이지](#)에서 선택한 원하는 네트워크 설계에 따라 각 디바이스에 대해 페일오버 인터페이스를 적절하게 연결합니다(스위치에 연결하거나 인터페이스를 서로 직접 연결).
- b) 별도의 상태 링크를 사용하는 경우에는 각 디바이스에 대해 스테이트풀 장애 조치 인터페이스도 적절하게 연결합니다.
- c) 각 디바이스에 차례로 로그인한 다음, **Device(디바이스) > Interface(인터페이스)**로 이동합니다. 각 인터페이스를 수정하고 인터페이스 이름 또는 IP 주소가 구성되어 있지 않는지 확인합니다.

이름이 지정된 인터페이스가 구성되어 있으면 보안 영역에서 해당 인터페이스를 제거하고 다른 컨피그레이션을 삭제해야 이름을 삭제할 수 있습니다. 이름 삭제에 실패하면 오류 메시지를 검사하여 수행해야 하는 기타 변경 작업을 확인합니다.

- 단계 6 기본 디바이스에서 나머지 데이터 인터페이스를 연결하고 디바이스를 구성합니다.
- Device(디바이스) > Interface(인터페이스)**를 선택하고 통과 트래픽에 사용되는 각 인터페이스를 수정한 다음 기본 고정 IP 주소를 구성합니다.
 - 보안 영역에 인터페이스를 추가하고 연결된 네트워크에서 트래픽을 처리하는 데 필요한 기본 정책을 구성합니다. 예시 컨피그레이션은 **모범 사례: Threat Defense의 사용 사례**에 나와 있는 주제를 참조하십시오.
 - 컨피그레이션을 구축합니다.
- 단계 7 **HA의 소프트웨어 요구 사항, 10 페이지**에 설명되어 있는 모든 요구 사항을 충족하는지 확인합니다.
- 단계 8 라이선싱이 일치하는지(등록됨 또는 평가 모드) 확인합니다. 자세한 내용은 **HA의 라이선스 요구 사항, 11 페이지**를 참고하십시오.
- 단계 9 보조 디바이스에서 나머지 데이터 인터페이스를 기본 디바이스의 해당 인터페이스와 동일한 네트워크에 연결합니다. 인터페이스를 구성하지는 마십시오.
- 단계 10 각 디바이스에서 **Device(디바이스) > System Settings(시스템 설정) > Cloud Services(클라우드 서비스)**를 선택하고 설정이 동일한지 확인합니다.

이제 기본 디바이스에서 고가용성을 구성할 준비가 되었습니다.

고가용성을 위한 기본 유닛 구성

액티브/스탠바이 고가용성 쌍을 설정하려면 먼저 기본 디바이스를 구성해야 합니다. 기본 디바이스는 정상적인 상황에서 액티브 상태로 운영할 유닛입니다. 보조 디바이스는 기본 유닛이 사용 불가능 상태가 될 때까지 스탠바이 모드로 유지됩니다.

기본으로 지정할 디바이스를 선택한 다음 해당 디바이스에서 **device manager**에 로그인하여 이 절차를 수행합니다.



참고 고가용성 쌍을 설정한 후 이 절차에서 설명하는 컨피그레이션을 수정하려면 해당 쌍을 해제해야 합니다.

시작하기 전에

페일오버 및 스테이트풀 페일오버 링크에 대해 구성하는 인터페이스에 이름이 지정되어 있지 않은지 확인합니다. 이러한 인터페이스에 현재 이름이 지정되어 있는 경우 보안 영역 개체를 포함하여 해당 이름을 사용하는 정책에서 인터페이스를 제거한 다음, 인터페이스를 수정하여 이름을 삭제해야 합니다. 또한 인터페이스는 패시브 모드가 아닌 라우팅 모드여야 합니다. 이러한 인터페이스는 HA 컨피그레이션 전용이어야 하며 다른 용도로는 사용할 수 없습니다.

보류 중인 변경 사항이 있는 경우 변경 사항을 구축해야 HA를 구성할 수 있습니다.

프로시저

단계 1 디바이스를 클릭합니다.

단계 2 디바이스 요약 오른쪽의 **High Availability**(고가용성) 옆에 있는 **Configure**(구성)를 클릭합니다.

디바이스에서 HA를 처음 구성하는 경우 그룹이 다음과 같이 표시됩니다.



단계 3 High Availability(고가용성) 페이지에서 **Primary Device**(기본 디바이스) 확인란을 클릭합니다.

보조 디바이스가 이미 구성되어 있으며 클립보드에 컨피그레이션을 복사한 경우 **Paste from Clipboard**(클립보드에서 붙여넣기) 버튼을 클릭하여 컨피그레이션을 붙여넣을 수 있습니다. 이렇게 하면 필드가 적절한 값으로 업데이트되며, 그러면 해당 값을 확인할 수 있습니다.

단계 4 **Failover Link**(페일오버 링크) 속성을 구성합니다.

페일오버 쌍의 두 유닛은 페일오버 링크를 통해 지속적으로 통신하여 각 유닛의 작동 상태를 확인하고 컨피그레이션 변경 사항을 동기화합니다. 자세한 내용은 [페일오버 링크, 4 페이지](#)를 참고하십시오.

- **Physical Interface**(물리적 인터페이스) - 페일오버 링크로 사용할 보조 디바이스에 연결한 인터페이스를 선택합니다. 이 인터페이스에는 이름이 지정되어 있지 않아야 합니다.

EtherChannel 인터페이스를 장애 조치 또는 상태 링크로 사용하는 경우, 고가용성을 설정하기 전에 동일한 ID 및 멤버 인터페이스를 사용하는 동일한 EtherChannel이 두 디바이스에 있는지 확인해야 합니다. EtherChannel이 일치하지 않는 경우에는 HA를 비활성화하고 이전의 보조 유닛에서 구성을 수정해야 합니다. 패킷의 오류를 방지하기 위해 EtherChannel에서는 하나의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다. 장애 조치 링크로 사용 중인 경우 EtherChannel 컨피그레이션을 변경할 수 없습니다.
- **Type**(유형) - 인터페이스에 사용할 주소(IPv4 또는 IPv6)를 선택합니다. 한 가지 유형의 주소만 구성할 수 있습니다.
- **Primary IP**(기본 IP) - 이 디바이스의 인터페이스 IP 주소를 입력합니다. 예를 들어 192.168.10.1을 입력합니다. IPv6 주소의 경우에는 2001:a0a:b00::a0a:b70/64와 같이 표준 표기법의 접두사 길이를 포함해야 합니다.
- **Secondary IP**(보조 IP) - 보조 디바이스의 인터페이스에 대해 링크 반대쪽에 구성해야 하는 IP 주소를 입력합니다. 해당 주소는 기본 주소와 같은 서브넷에 있어야 하며 기본 주소와는 달라야 합니다. 예를 들어 192.168.10.2 또는 2001:a0a:b00::a0a:b71/64를 입력합니다.
- **Netmask**(넷마스크)(IPv4 주소에만 해당) - 기본/보조 IP 주소의 서브넷 마스크를 입력합니다.

단계 5 스테이트풀 페일오버 링크 속성을 구성합니다.

시스템은 상태 링크를 사용해 연결 상태 정보를 스탠바이 디바이스에 전달합니다. 페일오버 수행 시에 스탠바이 유닛은 이 정보를 사용하여 기존 연결을 유지할 수 있습니다. 같은 링크를 페일오버 링크로 사용하거나 별도의 링크를 구성할 수 있습니다.

- **Use the Same Interface as the Failover Link**(페일오버 링크와 같은 인터페이스 사용) - 페일오버 및 스테이트풀 페일오버 통신에 단일 링크를 사용하려는 경우 이 옵션을 선택합니다. 이 옵션을 선택하는 경우 다음 단계를 계속 진행합니다.
- **Physical Interface**(물리적 인터페이스) - 별도의 스테이트풀 페일오버 링크를 사용하려는 경우 스테이트풀 페일오버 링크로 사용할 보조 디바이스에 연결한 인터페이스를 선택합니다. 이 인터페이스에는 이름이 지정되어 있지 않아야 합니다. 그런 다음, 다음의 속성을 구성합니다.
 - **Type**(유형) - 인터페이스에 사용할 주소(IPv4 또는 IPv6)를 선택합니다. 한 가지 유형의 주소만 구성할 수 있습니다.
 - **Primary IP**(기본 IP) - 이 디바이스의 인터페이스 IP 주소를 입력합니다. 해당 주소는 페일오버 링크에 사용한 주소와 다른 서브넷에 있어야 합니다. 예를 들어 192.168.11.1를 입력합니다. IPv6 주소의 경우에는 2001:a0a:b00:a::a0a:b70/64와 같이 표준 표기법의 접두사 길이를 포함해야 합니다.
 - **Secondary IP**(보조 IP) - 보조 디바이스의 인터페이스에 대해 링크 반대쪽에 구성해야 하는 IP 주소를 입력합니다. 해당 주소는 기본 주소와 같은 서브넷에 있어야 하며 기본 주소와는 달라야 합니다. 예를 들어 192.168.11.2 또는 2001:a0a:b00:a::a0a:b71/64를 입력합니다.
 - **Netmask**(넷마스크)(IPv4 주소에만 해당) - 기본/보조 IP 주소의 서브넷 마스크를 입력합니다.

단계 6 (선택 사항). 디바이스 쌍의 두 유닛 간 통신을 암호화하려면 **IPsec Encryption Key**(IPsec 암호화 키) 문자열을 입력합니다.

보조 노드에서 정확히 동일한 키를 구성해야 하므로 입력하는 문자열을 적어 두십시오.

키를 입력하지 않으면 페일오버 및 스테이트풀 페일오버 링크의 모든 통신에는 일반 텍스트가 사용됩니다. 인터페이스 간에 다이렉트 케이블 연결을 사용하지 않는 경우 보안 문제가 발생할 수 있습니다.

참고 평가 모드에서 HA 페일오버 암호화를 구성하는 경우 시스템은 암호화에 DES를 사용합니다. 그런 다음 내보내기 호환 계정을 사용하여 디바이스를 등록하면 디바이스는 재부팅 후 AES를 사용합니다. 따라서 업그레이드를 설치한 후를 포함하여 어떤 이유로든 시스템을 재부팅하면 피어가 통신할 수 없으며 두 유닛이 모두 활성 유닛이 됩니다. 디바이스를 등록할 때까지는 암호화를 구성하지 않는 것이 좋습니다. 평가 모드에서 구성하는 경우 디바이스를 등록하기 전에 암호화를 제거하는 것이 좋습니다.

단계 7 Activate HA(HA 활성화)를 클릭합니다.

시스템이 디바이스에 컨피그레이션을 즉시 구축합니다. 따라서 구축 작업을 시작할 필요가 없습니다. 컨피그레이션이 저장되었으며 구축이 진행 중이라는 메시지가 표시되지 않으면 페이지 위쪽으로 스크롤하여 오류 메시지를 확인합니다.

컨피그레이션은 클립보드에도 복사됩니다. 이 복사본을 사용하면 보조 유닛을 빠르게 구성할 수 있습니다. 보안 강화를 위해 암호화 키는 클립보드 복사본에 포함되지 않습니다.

컨피그레이션이 완료되면 수행해야 하는 다음 단계를 설명하는 메시지가 표시됩니다. 해당 정보를 확인한 후 **Got It**(확인)을 클릭합니다.

이 시점에서 High Availability(고가용성) 페이지가 표시되며 디바이스 상태는 "Negotiating(협상 중)"이라고 나타나야 합니다. 상태는 피어를 구성하기 전에 Active(활성)로 전환됩니다. 피어를 구성하기 전까지는 Failed(장애 발생)로 표시됩니다.

PRIMARY DEVICE
Current Device Mode: **Active**  Peer: **Failed** 

이제 보조 유닛을 구성할 수 있습니다. [고가용성을 위한 보조 유닛 구성, 19 페이지](#)의 내용을 참조하십시오.

참고 선택한 인터페이스는 직접 구성되지 않습니다. 하지만 CLI에서 **show interface**를 입력하면 인터페이스가 지정한 IP 주소를 사용 중임을 확인할 수 있습니다. 인터페이스 이름은 "failover-link"로 지정되며 별도의 상태 링크를 구성하는 경우에는 "stateful-failover-link"로 지정됩니다.

고가용성을 위한 보조 유닛 구성

액티브/스탠바이 고가용성용 기본 디바이스를 구성한 후에는 보조 디바이스를 구성해야 합니다. 해당 디바이스에서 device manager에 로그인하여 다음 절차를 수행합니다.



참고 고가용성 컨피그레이션을 기본 디바이스에서 클립보드로 아직 복사하지 않은 경우 이를 복사합니다. 데이터를 수동으로 입력하는 것보다 복사/붙여넣기를 사용하여 보조 디바이스를 구성하는 것이 훨씬 더 쉽습니다.

프로시저

단계 1 디바이스를 클릭합니다.

단계 2 디바이스 요약 오른쪽의 **High Availability(고가용성)** 옆에 있는 **Configure(구성)**를 클릭합니다.

디바이스에서 HA를 처음 구성하는 경우 그룹이 다음과 같이 표시됩니다.



단계 3 High Availability(고가용성) 페이지에서 **Secondary Device(보조 디바이스)** 확인란을 클릭합니다.

단계 4 다음 중 하나를 수행합니다.

- 쉬운 방법 - **Paste from Clipboard(클립보드에서 붙여넣기)** 버튼을 클릭하고 컨피그레이션에 붙여넣은 다음 **OK(확인)**를 클릭합니다. 이렇게 하면 필드가 적절한 값으로 업데이트되며, 그러면 해당 값을 확인할 수 있습니다.
- 수동 방법 - 페일오버 및 스테이트풀 페일오버 링크를 직접 구성합니다. 기본 디바이스에 입력한 것과 정확히 동일한 설정을 보조 디바이스에 입력합니다.

단계 5 기본 디바이스에서 **IPSec Encryption Key**(IPSec 암호화 키)를 구성한 경우에는 보조 디바이스에 대해 정확히 동일한 키를 입력합니다.

단계 6 **Activate HA**(HA 활성화)를 클릭합니다.

시스템이 디바이스에 컨피그레이션을 즉시 구축합니다. 따라서 구축 작업을 시작할 필요가 없습니다. 컨피그레이션이 저장되었으며 구축이 진행 중이라는 메시지가 표시되지 않으면 페이지 위쪽으로 스크롤하여 오류 메시지를 확인합니다.

컨피그레이션이 완료되면 HA를 구성했다는 메시지가 표시됩니다. **Got It**(확인)을 클릭하여 메시지를 해제합니다.

이 시점에서 **High Availability**(고가용성) 페이지가 표시되며 디바이스 상태에는 디바이스가 보조 디바이스임이 표시되어야 합니다. 기본 디바이스에 정상적으로 조인한 경우 디바이스는 기본 디바이스와 동기화되며, 최종적으로 이 디바이스의 모드가 **Standby**(스탠바이)로 설정되고 피어는 **Active**(액티브)로 설정되어야 합니다.

SECONDARY DEVICE
Current Device Mode: **Standby**  Peer Device: **Active**

참고 선택한 인터페이스는 직접 구성되지 않습니다. 하지만 CLI에서 **show interface**를 입력하면 인터페이스가 지정한 IP 주소를 사용 중임을 확인할 수 있습니다. 인터페이스 이름은 "failover-link"로 지정되며 별도의 상태 링크를 구성하는 경우에는 "stateful-failover-link"로 지정됩니다.

상태 모니터링을 위한 페일오버 기준 구성

고가용성 컨피그레이션의 유닛은 자체 모니터링을 통해 전반적인 상태와 인터페이스 상태를 확인합니다.

페일오버 기준은 피어에서 장애가 발생했는지 확인하는 상태 모니터링 메트릭을 정의합니다. 기준을 위반하는 유닛이 액티브 피어이면 스탠바이 유닛으로 페일오버를 트리거합니다. 기준을 위반하는 유닛이 스탠바이 피어이면 해당 유닛은 장애 발생 상태로 표시되며 페일오버에 사용할 수 없게 됩니다.

페일오버 기준은 액티브 디바이스에서만 구성할 수 있습니다.

다음 표에는 페일오버를 트리거하는 이벤트 및 관련 장애 탐지 타이밍이 나와 있습니다.

표 2: 페일오버 기준에 따른 페일오버 시간

페일오버를 트리거하는 이벤트	최소	기본	최대
액티브 유닛의 전원이 중단되거나 정상적인 작동이 중지됩니다.	800밀리초	15초	45초
액티브 유닛 인터페이스의 물리적 링크가 중단됩니다.	500밀리초	5초	15초

페일오버를 트리거하는 이벤트	최소	기본	최대
액티브 유닛 인터페이스가 작동하지만 연결 문제로 인해 인터페이스 테스트가 실행됩니다.	5초	25초	75초

다음 주제에서는 페일오버 상태 모니터링 기준을 맞춤 설정하는 방법과 시스템이 인터페이스를 테스트하는 방법을 설명합니다.

피어 유닛 상태 모니터링 페일오버 기준 구성

고가용성 컨피그레이션의 각 피어는 hello 메시지를 사용해 페일오버 링크를 모니터링하여 다른 유닛의 상태를 확인합니다. 페일오버 링크에서 hello 메시지가 유닛에 3번 연속으로 수신되지 않는 경우, 유닛에서는 페일오버 링크를 비롯한 각 데이터 인터페이스에 LANTEST 메시지를 전송하여 피어의 응답 여부를 검증합니다. 디바이스에서 취하는 조치는 다른 유닛의 응답에 따라 달라집니다.

- 디바이스가 페일오버 링크에서 응답을 수신하는 경우 디바이스는 페일오버를 수행하지 않습니다.
- 디바이스가 페일오버 링크에서는 응답을 수신하지 못했으나 데이터 인터페이스에서는 응답을 수신한 경우 유닛이 페일오버를 수행하지 않습니다. 페일오버 링크가 실패한 것으로 표시됩니다. 페일오버 링크가 중단된 동안에는 유닛에서 스탠바이 유닛으로 페일오버할 수 없으므로 최대한 빨리 페일오버 링크를 복원해야 합니다.
- 디바이스가 어떤 인터페이스에서도 응답을 받지 못한 경우 스탠바이 유닛은 액티브 모드로 전환되고 다른 유닛을 장애 발생 상태로 분류합니다.

hello 메시지의 폴링 및 대기 시간을 구성할 수 있습니다.

프로시저

단계 1 액티브 디바이스에서 **Device**(디바이스)를 클릭합니다.

단계 2 디바이스 요약의 오른쪽에서 **High Availability**(고가용성) 링크를 클릭합니다.

High Availability(고가용성) 페이지의 오른쪽 열에 Failover Criteria(페일오버 기준)가 나열됩니다.

단계 3 Peer Timing Configuration(피어 타이밍 컨피그레이션)을 정의합니다.

이러한 설정에 따라 액티브 디바이스가 스탠바이 디바이스로 페일오버할 수 있는 속도가 결정됩니다. 폴링 시간이 빠를수록 디바이스에서 더 빨리 장애를 탐지하고 페일오버를 더 빨리 트리거할 수 있습니다. 그러나 감지 기능이 빨라지면 네트워크에 일시적으로 정체 현상이 일어났을 때 불필요한 전환이 발생할 수 있습니다. 기본 설정은 대부분의 상황에 적합합니다.

한 차례의 폴링 기간 동안 유닛이 페일오버 인터페이스에서 hello 패킷을 수신하지 않은 경우, 나머지 인터페이스 전체에 추가 테스트가 이루어집니다. 대기 시간에도 피어 유닛의 응답이 없을 경우 그 유닛에 오류가 발생한 것으로 간주하며, 오류가 발생한 유닛이 활성 유닛이었다면 대기 유닛이 활성 유닛으로 전환합니다.

- **Poll Time**(폴링 시간) - hello 메시지 간의 시간입니다. 1~15초 또는 200~999밀리초를 입력합니다. 기본값은 1초입니다.
- **Hold Time**(대기 시간) - 유닛이 페일오버 링크에서 hello 메시지를 수신해야 하는 시간입니다. 이 시간이 지나면 피어 유닛은 장애 발생 상태로 선언됩니다. 대기 시간은 폴링 시간의 3배 이상이어야 합니다. 1~45초 또는 800~999밀리초를 입력합니다. 기본값은 15초입니다.

단계 4 **Save**(저장)를 클릭합니다.

인터페이스 상태 모니터링 페일오버 기준 구성

사용 중인 디바이스 모델에 따라 최대 211개의 인터페이스를 모니터링할 수 있습니다. 중요한 인터페이스를 모니터링해야 합니다. 중요 네트워크 간의 처리량을 확인하는 인터페이스를 예로 들 수 있습니다. 인터페이스용 스텐바이 IP 주소를 구성하는 경우 및 인터페이스가 항상 작동해야 하는 경우에만 인터페이스를 모니터링합니다.

2번의 폴링 기간 동안 모니터링된 인터페이스에 대한 hello 메시지가 유닛에 수신되지 않을 경우 인터페이스 테스트가 실행됩니다. 인터페이스에 대한 모든 인터페이스 테스트가 실패하였으나 다른 유닛에 있는 이 동일한 인터페이스에서는 지속적으로 트래픽을 전달할 수 있는 경우, 해당 인터페이스는 오류가 발생한 것으로 간주합니다. 오류가 발생한 인터페이스의 임계값이 충족될 경우 페일오버가 실행됩니다. 다른 유닛의 인터페이스에서도 모든 네트워크 테스트에 실패할 경우, 두 인터페이스 모두 "Unknown(알 수 없음)" 상태가 되며 페일오버 한도에 합산되지 않습니다.

트래픽이 수신될 경우 인터페이스는 다시 작동을 시작합니다. 인터페이스 오류 임계값이 더 이상 충족되지 않을 경우 장애가 발생한 디바이스는 스텐바이 모드로 돌아갑니다.

CLI 또는 CLI 콘솔에서 **show monitor-interface** 명령을 사용하여 인터페이스 HA 상태를 모니터링할 수 있습니다. 자세한 내용은 [HA 모니터링 인터페이스의 상태 모니터링, 39 페이지](#)를 참고하십시오.



참고 인터페이스가 중단될 때 페일오버의 경우 계속 유닛 문제로 간주됩니다. 유닛에서 인터페이스가 중단되었음을 탐지하면 인터페이스 대기 시간까지 기다리지 않고 페일오버가 즉시 수행됩니다(기본 임계값인 1개 인터페이스를 유지하는 경우). 인터페이스 대기 시간은 피어에서 hello 패킷이 수신되지 않더라도 유닛이 인터페이스 상태를 정상으로 간주하는 경우에만 유용합니다.

시작하기 전에

기본적으로 모든 명명된 물리적 인터페이스는 HA 모니터링 대상으로 선택됩니다. 따라서 중요하지 않은 물리적 인터페이스에서는 모니터링을 비활성화해야 합니다. 하위 인터페이스 또는 브리지 그룹의 경우 모니터링을 수동으로 활성화해야 합니다.

인터페이스 모니터링을 완전히 비활성화하고 인터페이스 오류로 인한 페일오버를 방지하려는 경우, HA 모니터링에 대해 활성화된 인터페이스가 없는지 확인하기만 하면 됩니다.

프로시저

단계 1 액티브 디바이스에서 **Device**(디바이스)를 클릭합니다.

단계 2 디바이스 요약의 오른쪽에서 **High Availability**(고가용성) 링크를 클릭합니다.

High Availability(고가용성) 페이지의 오른쪽 열에 Failover Criteria(페일오버 기준)가 나열됩니다.

단계 3 **Interface Failure Threshold**(인터페이스 오류 임계값)를 정의합니다.

장애가 발생한 인터페이스의 수가 임계값에 도달하면 유닛은 자체 상태를 장애 발생으로 표시합니다. 해당 유닛이 액티브 유닛인 경우 스탠바이 유닛으로 페일오버를 수행합니다. 또한 해당 유닛이 스탠바이 유닛인 경우에는 자체 상태를 장애 발생으로 표시하므로 액티브 유닛이 해당 유닛을 페일오버에 사용할 수 있는 유닛으로 간주하지 않습니다.

이 기준을 설정할 때는 모니터링 중인 인터페이스 수를 고려합니다. 예를 들어 인터페이스 2개에서만 모니터링을 활성화하는 경우에는 임계값(인터페이스 10개)에 도달하지 않습니다. 인터페이스 속성을 수정할 때 **Advanced Options**(고급 옵션) 탭에서 **Enable for HA Monitoring**(HA 모니터링에 대해 활성화) 옵션을 선택하여 인터페이스에 대해 모니터링을 구성합니다.

기본적으로는 모니터링하는 인터페이스 하나에서 장애가 발생하면 유닛은 자체 상태를 장애 발생으로 표시합니다.

다음의 **Failover Criteria**(페일오버 기준) 옵션 중 하나를 선택하여 인터페이스 오류 임계값을 설정할 수 있습니다.

- **Number of failed interfaces exceeds**(장애 발생 인터페이스의 수가 다음 값을 초과함) - 인터페이스의 원시 수를 입력합니다. 기본값은 1입니다. 최대값은 실제로 디바이스 모델에 따라 달라지며 모델별로 다를 수 있지만 211보다 큰 값은 입력할 수 없습니다. 이 기준을 사용하는 경우 디바이스가 지원하는 것보다 큰 수를 입력하면 구축 오류가 발생합니다. 오류 발생 시에는 더 작은 숫자를 입력하거나 퍼센트를 대신 사용해 보십시오.
- **Percentage of failed interfaces exceeds**(장애 발생 인터페이스의 퍼센트가 다음 값을 초과함) - 1~100 사이의 숫자를 입력합니다. 예를 들어 인터페이스 10개를 모니터링하는 데 50%를 입력하는 경우 인터페이스 5개에서 장애가 발생하면 디바이스가 자체 상태를 장애 발생으로 표시합니다.

단계 4 **Interface Timing Configuration**(인터페이스 타이밍 컨피그레이션)을 정의합니다.

이러한 설정은 인터페이스가 실패한 경우 활성 디바이스를 얼마나 빨리 확인할 수 있는지를 결정합니다. 폴링 시간이 더 빨라지면 디바이스는 인터페이스 오류를 더 빨리 감지할 수 있습니다. 그러나 탐지 속도가 너무 빠르면 사용 중인 인터페이스가 실제로 정상인 경우에도 장애 발생으로 표시하여 페일오버가 불필요하게 자주 발생할 수 있습니다. 기본 설정은 대부분의 상황에 적합합니다.

인터페이스 링크가 중단되면 인터페이스 테스트가 시행되지 않으며, 장애가 발생한 인터페이스 수가 구성된 인터페이스 페일오버 임계값과 일치하거나 이를 초과할 경우 한 차례의 인터페이스 폴링 기간 동안에만 스탠바이 유닛이 액티브 상태가 됩니다.

- **Poll Time**(폴링 시간) - hello 패킷이 데이터 인터페이스에서 전송되는 빈도입니다. 1~15초 또는 500~999밀리초를 입력합니다. 기본값은 5초입니다.

- **Hold Time**(대기 시간) - 대기 시간은 인터페이스가 장애 발생 상태로 표시될 때 hello 패킷이 손실될 때까지 걸리는 시간을 결정합니다. 5~75초를 입력합니다. 대기 시간은 폴링 시간보다 5배 적게 입력할 수 없습니다.

단계 5 **Save**(저장)를 클릭합니다.

단계 6 모니터링할 각 인터페이스에 대해 HA 모니터링을 활성화합니다.

- a) **Device**(디바이스) > **Interfaces**(인터페이스)를 선택합니다.

인터페이스를 모니터링하는 경우 Monitor for HA(HA에 대해 모니터링) 옆에 Enabled(활성화)가 표시됩니다.

- b) 모니터링 상태를 변경할 인터페이스에 대해 수정 아이콘(🔍)을 클릭합니다.

페일오버 또는 스테이트풀 페일오버 인터페이스는 수정할 수 없습니다. 이러한 인터페이스에는 인터페이스 모니터링이 적용되지 않습니다.

- c) **Advanced Options**(고급 옵션) 탭을 클릭합니다.

- d) **Enable for HA Monitoring**(HA 모니터링에 대해 활성화) 확인란을 원하는 대로 선택하거나 선택 취소합니다.

- e) **OK**(확인)를 클릭합니다.

단계 7 (선택 사항, 권장함.) 모니터링하는 인터페이스에 대해 스탠바이 IP 주소와 MAC 주소를 구성합니다. [스탠바이 IP 및 MAC 주소 구성, 25 페이지](#)의 내용을 참조하십시오.

시스템이 인터페이스 상태를 테스트하는 방법

시스템은 사용자가 고가용성 상태를 확인하기 위해 모니터링하는 인터페이스를 지속적으로 테스트합니다. 인터페이스 테스트에 사용되는 주소는 사용자가 구성하는 주소 유형을 기준으로 합니다.

- 인터페이스에 IPv4 및 IPv6 주소가 모두 구성되어 있으면 디바이스는 IPv4 주소를 사용하여 상태 모니터링을 수행합니다.
- 인터페이스에 IPv6 주소만 구성되어 있으면 디바이스는 ARP 대신 IPv6 네이버 검색을 사용하여 상태 모니터링 테스트를 수행합니다. 브로드캐스트 ping 테스트의 경우 디바이스는 IPv6 모든 노드 주소를 사용합니다(FE02::1).

시스템은 각 유닛에서 다음 테스트를 수행합니다.

1. 링크 작동/중단 테스트 - 인터페이스 상태에 대한 테스트입니다. 링크 작동/중단 테스트는 인터페이스가 중단되었는지를 나타내며, 인터페이스가 중단된 경우 유닛은 인터페이스에 장애가 발생한 것으로 간주합니다. 상태가 Up(작동 중)인 경우 유닛은 네트워크 활동 테스트를 수행합니다.
2. 네트워크 활동 테스트 - 수신된 네트워크 활동 테스트입니다. 이 테스트의 목적은 LANTEST 메시지를 사용하는 네트워크 트래픽을 생성하여 어떤 유닛에서 오류가 발생했는지 확인하는 것입니다. 테스트를 시작할 때마다 각 유닛에서는 해당 인터페이스에 대한 수신된 패킷 수를 지웁니다. 유닛에서 테스트 동안(최대 5초) 임의의 패킷을 수신하는 즉시, 인터페이스는 작동 중으로 간주됩니다. 한 유닛에는 트래픽이 수신되고 다른 유닛에는 수신되지 않을 경우, 트래픽이 수신되지

않은 유닛은 오류가 발생한 것으로 간주합니다. 어떤 유닛도 트래픽을 받지 못했으면 유닛은 ARP 테스트를 시작합니다.

3. ARP 테스트 - 최근에 얻은 항목 2개의 유닛 ARP 캐시를 읽는 테스트입니다. 유닛에서는 한 번에 하나씩 ARP 요청을 이러한 디바이스에 전송하여 네트워크 트래픽을 자극합니다. 각 요청 후 유닛에서는 최대 5초 동안 수신된 모든 트래픽의 수를 셉니다. 트래픽이 수신된 경우 해당 인터페이스는 제대로 작동 중인 것으로 간주합니다. 트래픽이 수신되지 않으면 ARP 요청이 다음 디바이스에 전송됩니다. 목록 마지막까지 트래픽이 수신되지 않은 경우 유닛은 ping 테스트를 시작합니다.
4. 브로드캐스트 ping 테스트 - 브로드캐스트 ping 요청을 전송하는 작업으로 이루어진 ping 테스트입니다. 그런 다음 유닛에서는 최대 5초 동안 수신된 모든 패킷의 수를 셉니다. 이 간격 동안 언제라도 수신된 패킷이 있을 경우 인터페이스가 작동 중인 것으로 간주되며 테스트가 중지됩니다. 모든 트래픽이 수신되지 않으면, 테스트는 ARP 테스트와 함께 다시 시작됩니다.

스탠바이 IP 및 MAC 주소 구성

인터페이스를 구성할 때는 동일한 네트워크에서 액티브 IP 주소 및 스탠바이 IP 주소를 지정할 수 있습니다. 스탠바이 주소는 지정하는 것이 좋지만 필수 항목은 아닙니다. 스탠바이 IP 주소가 없으면 액티브 유닛이 네트워크 테스트를 수행하여 스탠바이 인터페이스 상태를 확인할 수 없으며 링크 상태만 추적할 수 있습니다. 관리 목적으로 해당 인터페이스에서 스탠바이 유닛에 연결할 수도 없습니다.

1. 기본 유닛에서 페일오버가 수행될 때 보조 유닛에서는 기본 유닛의 IP 주소와 MAC 주소를 가정하고 트래픽 전달을 시작합니다.
2. 이제 스탠바이 상태가 된 유닛에서는 스탠바이 IP 주소와 MAC 주소를 인수합니다.

네트워크 디바이스에서는 MAC-IP 주소 쌍의 변화가 감지되지 않으므로, 네트워크 어디에서도 ARP 항목의 변경이나 시간 초과가 발생하지 않습니다.

기본 유닛을 감지하지 않고 부팅되는 보조 유닛은 액티브 유닛이 되며 기본 유닛의 MAC 주소를 알지 못하므로 고유한 MAC 주소를 사용합니다. 그러나 기본 유닛이 사용 가능해지면 보조(액티브) 유닛이 MAC 주소를 기본 유닛의 주소로 변경하므로 네트워크 트래픽이 중단될 수 있습니다. 마찬가지로, 기본 유닛을 새 하드웨어로 교체하면 새 MAC 주소가 사용됩니다.


시작 시 보조 유닛에 액티브 MAC 주소가 알려지므로 가상 MAC 주소에서는 이러한 중단을 방지하며, 새 기본 유닛 하드웨어가 사용될 경우에도 가상 MAC 주소는 그대로 유지됩니다. 가상 MAC 주소를 수동으로 구성할 수 있습니다.

가상 MAC 주소를 구성하지 않을 경우, 연결된 라우터에서 ARP 테이블을 지워 트래픽 흐름을 복원해야 할 수 있습니다. MAC 주소가 변경될 경우 위협 방지 디바이스에서는 고정 NAT 주소에 불필요한 ARP를 전송하지 않으므로, 연결된 라우터에서는 이러한 주소의 MAC 주소 변경을 알지 못합니다.

프로시저

단계 1 **Device**(디바이스) > **Interfaces**(인터페이스)를 선택합니다.

최소한 HA를 모니터링하는 인터페이스에 대해 스탠바이 IP 및 MAC 주소를 구성해야 합니다. 인터페이스를 모니터링하는 경우 Monitor for HA(HA에 대해 모니터링) 열에 Enabled(활성화)가 표시됩니다.

단계 2 스탠바이 주소를 구성할 인터페이스의 수정 아이콘()을 클릭합니다.

페일오버 또는 스테이트풀 페일오버 인터페이스는 수정할 수 없습니다. 고가용성을 구성할 때 이러한 인터페이스에 대해 IP 주소를 설정합니다.

단계 3 IPv4 Address(IPv4 주소) 및 IPv6 Address(IPv6 주소) 탭에서 스탠바이 IP 주소를 구성합니다.

스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다. 사용 중인 각 IP 버전에 대해 스탠바이 주소를 구성합니다.

단계 4 Advance Options(고급 옵션) 탭을 클릭하고 MAC 주소를 구성합니다.


시스템은 기본적으로 인터페이스에 대해 NIC(Network Interface Card)에 버닝된 MAC 주소를 사용합니다. 따라서 인터페이스의 모든 하위 인터페이스는 같은 MAC 주소를 사용하므로 하위 인터페이스별로 고유한 주소를 생성할 수 있습니다. 고가용성을 구성하는 경우에는 액티브/스탠바이 MAC 주소도 수동으로 구성하는 것이 좋습니다. MAC 주소를 정의하면 페일오버 시 네트워크에서 일관성을 유지할 수 있습니다.

- **MAC Address(MAC 주소)** - H.H.H. 형식의 MAC(Media Access Control) 주소입니다. 여기서 H는 16비트 16진수입니다. 예를 들어 MAC 주소 00-0C-F1-42-4C-DE는 00C.F142.4CDE로 입력합니다. MAC 주소에는 멀티캐스트 비트를 설정해서는 안 됩니다(즉, 왼쪽에서 두 번째 16진수는 홀수일 수 없음).
- **Standby MAC Address(스탠바이 MAC 주소)** - 고가용성에 사용할 주소입니다. 액티브 유닛이 페일오버되고 스탠바이 유닛이 액티브 상태가 되면, 네트워크 중단을 최소화하기 위해 새 액티브 유닛에서 액티브 MAC 주소를 사용하기 시작하고 기존 액티브 유닛은 스탠바이 주소를 사용합니다.

단계 5 OK(확인)를 클릭합니다.

고가용성 컨피그레이션 확인

고가용성 컨피그레이션을 완료한 후에는 디바이스 상태에 두 디바이스가 모두 작동하며 액티브/스탠바이 모드임이 표시됨을 확인합니다.

PRIMARY DEVICE
Current Device Mode: **Active**  Peer Device: **Standby**

다음 절차에 따라 고가용성 컨피그레이션이 작동함을 확인할 수 있습니다.

프로시저

- 단계 1 활성 유닛에서 FTP(예)를 사용하여 정상적으로 트래픽을 전달하여 다른 인터페이스의 호스트 간에 파일을 전송하는지 테스트합니다.
- 최소한 워크스테이션 하나에서 구성된 각 인터페이스에 연결되어 있는 시스템으로의 연결을 테스트합니다.
- 단계 2 다음 중 하나를 수행하여 액티브 유닛이 이제 스탠바이 유닛이 되도록 모드를 전환합니다.
- device manager에서 **Device(디바이스) > High Availability(고가용성)** 페이지의 기어 메뉴에 있는 **Switch Mode(모드 전환)**를 선택합니다.
 - 액티브 유닛의 CLI에 **no failover active**를 입력합니다.
- 단계 3 연결 테스트를 반복하여 고가용성 쌍의 다른 유닛을 통해서도 같은 연결을 설정할 수 있는지 확인합니다.
- 테스트가 실패하는 경우 다른 유닛의 동일 인터페이스와 같은 네트워크에 유닛 인터페이스를 연결했는지 확인합니다.
- High Availability(고가용성) 페이지에서 HA 상태를 확인할 수 있습니다. 유닛의 CLI 또는 CLI 콘솔을 사용해 **show failover** 명령을 입력하여 페일오버 상태를 확인할 수도 있습니다. 또한 **show interface** 명령을 사용하여 실패한 연결 테스트에서 사용한 인터페이스의 인터페이스 컨피그레이션을 확인합니다.
- 이러한 작업에서 문제가 식별되지 않는 경우 다른 단계를 수행할 수 있습니다. [고가용성 트러블슈팅\(페일오버\), 40 페이지](#)의 내용을 참조하십시오.
- 단계 4 작업을 완료한 후 모드를 전환하여 원래 액티브였던 유닛을 액티브 상태로 되돌릴 수 있습니다.

고가용성 관리

Device Summary(디바이스 요약) 페이지에서 **High Availability(고가용성)** 링크를 클릭하면 고가용성 쌍을 관리할 수 있습니다.



High Availability(고가용성) 페이지에는 다음 항목이 포함되어 있습니다.

- **Role and Mode Status(역할 및 모드 상태)** - 왼쪽 상태 영역에는 그룹에서 디바이스가 Primary(기본) 디바이스인지 아니면 Secondary(보조) 디바이스인지 표시됩니다. 모드는 이 디바이스의 상태(액티브/스탠바이) 또는 HA가 일시 중단되었는지 아니면 디바이스가 피어 디바이스 조인을 기다리고 있는지를 나타냅니다. 또한 피어 디바이스의 상태도 표시됩니다. 이 상태는 Active(액티브), Standby(스탠바이), Suspended(일시 중단됨) 또는 Failed(장애 발생) 중 하나일 수 있습니다. 예를 들어 기본 디바이스이자 액티브 디바이스에 로그인하는 경우, 보조 디바이스가 정상 상태

이며 필요 시 페일오버 준비가 되어 있다면 상태는 다음과 같이 표시됩니다. 피어 사이의 아이콘을 클릭하면 디바이스 간의 컨피그레이션 동기화 상태에 대한 정보를 가져올 수 있습니다.

PRIMARY DEVICE
Current Device Mode: **Active**  Peer Device: **Standby**

- **Last Failure Reason**(마지막 실패 사유) - 액티브 디바이스를 사용할 수 없게 되고 스탠바이 디바이스에 장애 조치를 수행하는 등의 이유로 HA(고가용성) 구성이 실패하는 경우, 마지막 실패 사유가 역할 및 모드 상태에 대한 상태 정보 아래에 표시됩니다. 이 메시지는 장애 조치 기록에서 파생됩니다.
- **Failover History**(페일오버 기록) 링크 - 이 링크를 클릭하면 디바이스 쌍에 포함된 디바이스 상태의 세부 기록을 확인할 수 있습니다. 시스템에서는 CLI 콘솔을 열고 **show failover history details** 명령을 실행합니다.
- **Deployment History**(구축 기록) 링크 - 이 링크를 클릭하면 구축 작업만 표시하도록 필터링된 이벤트를 포함하는 감사 로그로 이동하게 됩니다.
- 기어 버튼  - 이 버튼을 클릭하면 디바이스에 대해 작업을 수행할 수 있습니다.
 - **Suspend HA**(HA 일시 중단)/**Resume HA**(HA 다시 시작) - HA를 일시 중단하면 디바이스가 고가용성 쌍으로 작동하지 않게 되지만 HA 컨피그레이션은 제거되지 않습니다. 나중에 디바이스에서 HA를 다시 시작(다시 활성화)할 수 있습니다. 자세한 내용은 [고가용성 일시 중단 또는 다시 시작, 29 페이지](#)를 참조해 주십시오.
 - **Break HA**(HA 해제) - HA를 해제하면 두 디바이스에서 모두 고가용성 컨피그레이션이 제거되며 모두 독립형 디바이스로 돌아갑니다. 자세한 내용은 [고가용성 해제, 30 페이지](#)를 참조해 주십시오.
 - **Switch Mode**(모드 전환) - 모드를 전환하면 작업을 수행하는 디바이스에 따라 액티브 디바이스를 스탠바이 디바이스로, 또는 스탠바이 디바이스를 액티브 디바이스로 강제 설정할 수 있습니다. 자세한 내용은 [액티브 및 스탠바이 피어 전환\(강제 페일오버\), 31 페이지](#)를 참조해 주십시오.
- **High Availability Configuration**(고가용성 컨피그레이션) - 이 패널에는 페일오버 쌍의 컨피그레이션이 표시됩니다. **Copy to Clipboard**(클립보드에 복사) 버튼을 클릭하여 정보를 클립보드에 로드하고 보조 디바이스의 컨피그레이션에 정보를 붙여넣을 수 있습니다. 또한 기록을 위해 다른 파일로 복사할 수도 있습니다. 이 정보에는 IPsec 암호화 키를 정의했는지 여부가 표시되지 않습니다.



참고 HA용 인터페이스 컨피그레이션은 **Interfaces**(인터페이스) 페이지 (**Device**(디바이스) > **Interfaces**(인터페이스))에 반영되지 않습니다. HA 컨피그레이션에서 사용하는 인터페이스는 수정할 수 없습니다.

- **Failover Criteria**(페일오버 기준) - 이 패널에는 액티브 유닛에서 장애가 발생하여 스탠바이 유닛이 액티브 유닛으로 설정되어야 하는지 여부를 평가할 때 사용되는 상태 기준을 결정하는 설정이 포함되어 있습니다. 네트워크에 필요한 페일오버 성능을 얻을 수 있도록 이러한 기준을 조

정할 수 있습니다. 자세한 내용은 [상태 모니터링을 위한 페일오버 기준 구성, 20 페이지](#)를 참조해 주십시오.

다음 주제에서는 고가용성 컨피그레이션과 관련된 다양한 관리 작업을 설명합니다.

고가용성 일시 중단 또는 다시 시작

고가용성 쌍의 유닛을 일시 중단할 수 있습니다. 이렇게 하면 다음과 같은 경우에 유용합니다.

- 두 유닛이 모두 액티브-액티브인 상태에서 페일오버 링크의 통신을 수정해도 문제가 해결되지 않는 경우.
- 액티브 또는 스탠바이 유닛을 트러블슈팅하고 트러블슈팅 중에는 유닛을 페일오버하지 않으려는 경우.
- 스탠바이 디바이스에 소프트웨어 업그레이드를 설치하는 동안 페일오버를 방지하려는 경우.

고가용성을 일시 중단하면 디바이스 쌍이 더 이상 페일오버 유닛으로 동작하지 않게 됩니다. 현재 액티브 디바이스는 액티브 상태로 유지되어 모든 사용자 연결을 처리합니다. 그러나 페일오버 기준은 더 이상 모니터링되지 않으며 시스템은 현재 의사 스탠바이 디바이스로 페일오버되지 않습니다. 스탠바이 디바이스의 컨피그레이션은 보존되지만 해당 디바이스는 비활성 상태로 유지됩니다.

HA 일시 중단과 해제와 주요 차이점은 일시 중단된 HA 디바이스에서는 고가용성 컨피그레이션이 보존된다는 것입니다. 반면 HA를 해제하면 컨피그레이션이 지워집니다. 따라서 일시 중단된 시스템에서 HA를 다시 시작하는 옵션이 제공됩니다. 그러면 기존 컨피그레이션이 활성화되며 두 디바이스가 다시 페일오버 쌍으로 작동합니다.

액티브 유닛에서 고가용성을 일시 중단하면 액티브 유닛과 스탠바이 유닛 둘 다에서 컨피그레이션이 일시 중단됩니다. 스탠바이 유닛에서 고가용성을 일시 중단하는 경우에는 스탠바이 유닛에서만 고가용성이 일시 중단되며 액티브 유닛은 일시 중단된 유닛으로의 페일오버를 시도하지 않습니다.

Suspended(일시 중단됨) 상태인 유닛만 다시 시작할 수 있습니다. 이 유닛은 피어 유닛과 액티브/스탠바이 상태를 협상합니다.



참고 필요한 경우, **configure high-availability suspend** 명령을 입력하여 CLI에서 HA를 일시 중단할 수 있습니다. HA를 다시 시작하려면 **configure high-availability resume** 명령을 입력합니다.

시작하기 전에

device manager를 통해 고가용성을 일시 중단하면 유닛을 다시 로드하더라도 고가용성은 다시 시작할 때까지 일시 중단된 상태로 유지됩니다. 그러나 CLI를 통해 고가용성을 일시 중단하는 경우에는 일시 중단 상태가 일시적으로만 유지되며, 유닛을 다시 로드하면 고가용성 컨피그레이션이 자동으로 다시 시작되고 피어와의 액티브/스탠바이 상태 협상이 진행됩니다.

스탠바이 유닛에서 고가용성을 일시 중단하는 경우에는 액티브 유닛이 현재 구축 작업을 실행하고 있는지를 확인하십시오. 구축 작업이 진행 중일 때 모드를 전환하면 작업이 실패하고 컨피그레이션 변경 사항이 손실됩니다.

프로시저

단계 1 디바이스를 클릭합니다.

단계 2 디바이스 요약의 오른쪽에서 **High Availability**(고가용성) 링크를 클릭합니다.

단계 3 기어 아이콘(⚙️)에서 적절한 명령을 선택합니다.

- **Suspend HA(HA 일시 중단)** - 작업을 확인하라는 프롬프트가 표시 됩니다. 메시지를 확인하고 **OK**(확인)를 클릭합니다. HA 상태에 디바이스가 **Suspended**(일시 중단됨) 모드임이 표시됩니다.
- **Resume HA(HA 다시 시작)** - 작업을 확인하라는 프롬프트가 표시 됩니다. 메시지를 확인하고 **OK**(확인)를 클릭합니다. 유닛이 피어와 상태를 협상하고 나면 HA 상태가 정상(액티브 또는 스탠바이) 상태로 돌아갑니다.

고가용성 해제

두 디바이스가 더 이상 고가용성 쌍으로 작동하지 않도록 하려면 HA 컨피그레이션을 해제할 수 있습니다. HA를 해제하면 각 디바이스는 독립형 디바이스가 됩니다. 디바이스의 컨피그레이션은 다음과 같이 변경됩니다.

- 액티브 디바이스의 경우 해제 전의 전체 컨피그레이션이 유지되며 HA 컨피그레이션은 제거됩니다.
- 스탠바이 디바이스의 경우 HA 컨피그레이션과 함께 모든 인터페이스 컨피그레이션이 제거됩니다. 하위 인터페이스는 비활성화되지 않지만 모든 물리적 인터페이스는 비활성화됩니다. 디바이스에 로그인하여 디바이스를 재구성할 수 있도록 관리 인터페이스는 액티브 상태로 유지됩니다.



참고 또는 API Explorer에서 **BreakHAStatus** API 리소스를 사용하고 **interfaceOption** 속성을 사용함으로써 시스템에서 스탠바이 IP 주소를 사용하여 스탠바이 디바이스의 인터페이스를 재구성하도록 지시할 수 있습니다. 이러한 결과를 원하는 경우 API를 사용해야 합니다. **device manager**에서는 항상 인터페이스를 비활성화합니다. 시스템은 IP 주소를 재구성하지만 그 외에는 모든 인터페이스 옵션을 다시 구성하지 않으므로, 브레이크 이후에 변경 사항을 구축할 때까지 트래픽이 예상대로 작동하지 않을 수 있습니다.

HA 해제가 실제로 유닛에 미치는 영향은 해제를 수행할 때의 각 유닛의 상태에 따라 달라집니다.

- 유닛이 정상 액티브/스탠바이 상태라면 액티브 유닛에서 HA를 해제합니다. 이렇게 하면 HA 쌍의 두 디바이스에서 모두 HA 컨피그레이션이 제거됩니다. 스탠바이 유닛에서만 HA를 해제하려는 경우에는 해당 유닛에 로그인한 다음 먼저 HA를 일시 중단해야 HA를 해제할 수 있습니다.

- 스탠바이 유닛이 일시 중단 또는 장애 발생 상태인 경우, 액티브 유닛에서 HA를 해제하면 액티브 유닛에서만 HA 컨피그레이션이 제거됩니다. 그러므로 스탠바이 유닛에 로그인하여 해당 유닛에서도 HA를 해제해야 합니다.
- 피어가 아직 HA를 협상하거나 컨피그레이션을 동기화하는 중이라면 HA를 해제할 수 없습니다. 협상 또는 동기화가 완료되거나 시간이 초과될 때까지 기다리십시오. 시스템이 이 상태로 멈춘 것 같다면 HA를 일시 중단한 후에 해제할 수 있습니다.



참고 device manager를 사용할 때는 **configure high-availability disable** 명령을 사용하여 CLI에서 HA를 해제할 수 없습니다.

시작하기 전에

원하는 결과를 얻으려면 디바이스를 정상적인 액티브/스탠바이 상태로 설정하고 액티브 디바이스에서 이 작업을 수행합니다.

프로시저

단계 1 디바이스를 클릭합니다.

단계 2 디바이스 요약의 오른쪽에서 **High Availability(고가용성)** 링크를 클릭합니다.

단계 3 기어 아이콘(⚙)에서 **Break HA(HA 해제)**를 선택합니다.

단계 4 확인 메시지를 읽고 인터페이스를 비활성화하는 옵션을 선택할지 여부를 결정한 다음 **OK(확인)**를 클릭합니다.

스탠바이 유닛에서 HA를 해제하는 경우 인터페이스를 비활성화하는 옵션을 선택해야 합니다.

시스템은 이 디바이스와 피어 디바이스(가능한 경우)에서 모두 변경 사항을 즉시 구축합니다. 각 디바이스에서 구축이 완료되고 각 디바이스가 독립 유닛으로 설정되려면 몇 분 정도 걸릴 수 있습니다.

액티브 및 스탠바이 피어 전환(강제 페일오버)

작동 중인 고가용성 쌍(피어 하나는 액티브, 다른 하나는 스탠바이 상태임)의 액티브/스탠바이 모드를 전환할 수 있습니다. 예를 들어 소프트웨어 업그레이드를 설치하는 경우 업그레이드가 사용자 트래픽에 영향을 주지 않도록 액티브 유닛을 스탠바이로 전환할 수 있습니다.

액티브 또는 스탠바이 유닛에서 모드를 전환할 수는 있지만, 다른 유닛의 시점에서 볼 때 피어 유닛이 작동해야 합니다. 즉, 특정 유닛이 일시 중단되거나(먼저 HA를 다시 시작해야 함) 장애가 발생하는 경우에는 모드를 전환할 수 없습니다.



참고 필요한 경우에는 CLI에서 액티브 및 스탠바이 모드 간을 전환할 수 있습니다. 스탠바이 유닛에서 **failover active** 명령을 입력합니다. 액티브 유닛에서 **no failover active** 명령을 입력합니다.

시작하기 전에

모드를 전환하기 전에 액티브 유닛이 구축 작업을 수행하고 있지 않은지 확인합니다. 모드를 전환하기 전에 구축이 완료될 때까지 기다리십시오.

액티브 유닛에 보류 중인 구축되지 않은 변경 사항이 있는 경우 모드를 전환하기 전에 구축하십시오. 이렇게 하지 않으면 새 액티브 유닛에서 구축 작업을 실행하는 경우 변경 사항이 손실됩니다.

프로시저

단계 1 디바이스를 클릭합니다.

단계 2 디바이스 요약의 오른쪽에서 **High Availability**(고가용성) 링크를 클릭합니다.

단계 3 기어 아이콘(⚙️)에서 **Switch Mode**(모드 전환)를 선택합니다.

단계 4 확인 메시지를 읽고 **OK**(확인)를 클릭합니다.

시스템이 페일오버를 강제로 수행하여 액티브 유닛은 스탠바이 유닛이 되고 스탠바이 유닛은 새 활성 유닛이 됩니다.

페일오버 후 구축되지 않은 컨피그레이션 변경 사항 보존

고가용성 쌍의 유닛에서 컨피그레이션을 변경할 때 액티브 유닛의 컨피그레이션을 수정합니다. 그런 다음, 변경 사항을 구축하면 액티브 유닛과 스탠바이 유닛이 모두 새 컨피그레이션으로 업데이트 됩니다. 액티브 유닛이 기본 디바이스인지 아니면 보조 디바이스인지는 중요하지 않습니다.

그러나 구축되지 않은 변경 사항은 유닛 간에 동기화되지 않습니다. 구축되지 않은 변경 사항은 해당 변경을 수행한 유닛에서만 사용할 수 있습니다.

따라서 구축되지 않은 변경 사항이 있을 때 페일오버가 수행되면 새 액티브 유닛에서는 해당 변경 사항을 사용할 수 없습니다. 하지만 이제 스탠바이 상태의 유닛에 변경 사항이 그대로 유지됩니다.

구축되지 않은 변경 사항을 검색하려면 모드를 전환하여 페일오버를 강제로 수행하고 다른 유닛을 액티브 상태로 되돌려야 합니다. 새 액티브 유닛에 로그인하면 구축되지 않은 변경 사항을 사용할 수 있으며 구축할 수 있습니다. 이렇게 하려면 **High Availability**(고가용성) 설정 기어 메뉴(⚙️)에서 **Switch Modes**(모드 전환) 명령을 사용합니다.

다음 사항에 유의하십시오.

- 스탠바이 유닛에 구축되지 않은 변경 사항이 있는 상태에서 액티브 유닛의 변경 사항을 구축하면 스탠바이 유닛의 구축되지 않은 변경 사항은 지워지며 검색할 수 없게 됩니다.

- 스탠바이 유닛이 고가용성 쌍에 조인하면 스탠바이 유닛의 구축되지 않은 변경 사항은 지워집니다. 유닛이 쌍에 조인하거나 다시 조인할 때마다 컨피그레이션이 동기화됩니다.
- 구축되지 않은 변경 사항이 포함된 유닛에서 심각한 장애가 발생하여 해당 유닛을 교체하거나 이미지를 재설치해야 하는 경우에는 구축되지 않은 변경 사항이 영구적으로 손실됩니다.

고가용성 모드에서 라이선스 및 등록 변경

고가용성 쌍의 유닛은 라이선스 및 등록 상태가 동일해야 합니다. 이러한 상태를 변경하려면 다음을 수행해야 합니다.

- 액티브 유닛에서 선택적 라이선스를 활성화하거나 비활성화합니다. 그런 다음, 컨피그레이션을 구축하면 스탠바이 유닛이 필요한 라이선스를 요청하거나 해제합니다. 라이선스를 활성화하는 경우에는 Cisco Smart Software Manager 어카운트에 사용 가능한 라이선스가 충분한지 확인해야 합니다. 그렇지 않으면 각 유닛의 컴플라이언스 상태가 서로 다를 수 있습니다.
- 각 유닛을 개별적으로 등록하거나 등록 취소합니다. 유닛은 둘 다 평가 모드이거나 등록되어 있어야 정상적으로 작동합니다. 유닛을 다른 Cisco Smart Software Manager 어카운트에 등록할 수 있습니다. 단, 이러한 어카운트의 내보내기 제어 기능 설정 상태가 같아야 합니다(둘 다 활성화되어 있거나 비활성화되어 있어야 함). 유닛의 등록 상태가 불일치하는 경우에는 컨피그레이션 변경 사항을 구축할 수 없습니다.

HA IPsec 암호화 키 또는 HA 컨피그레이션 수정

액티브 유닛에 로그인하고 변경을 수행한 다음 변경 사항을 구축하면 페일오버 기준을 변경할 수 있습니다.

그러나 페일오버 링크에 사용되는 IPsec 암호 키를 변경해야 하거나, 페일오버 또는 스테이트풀 페일오버 링크의 인터페이스 또는 IP 주소를 변경해야 하는 경우에는 먼저 HA 구성을 해제해야 합니다. 그런 다음 새 암호화 키 또는 페일오버/스테이트풀 페일오버 링크 설정을 사용하여 기본 유닛과 보조 유닛을 다시 구성할 수 있습니다.

장애가 발생한 유닛을 정상 상태로 표시

고가용성 컨피그레이션의 유닛은 정기적 상태 모니터링으로 인해 장애 발생 상태로 표시될 수 있습니다. 해당 유닛이 정상 상태인 경우, 상태 모니터링 요구 사항을 다시 충족했을 때 정상 상태로 되돌려야 합니다. 정상 디바이스가 자주 장애 발생 상태로 표시되는 경우에는 피어 시간 제한을 늘리거나, 중요도가 낮은 인터페이스의 모니터링을 중지하거나, 인터페이스 모니터링 시간 제한을 변경할 수 있습니다.

CLI에서 **failover reset** 명령을 입력하면 장애 발생 상태로 표시된 유닛을 정상 상태로 강제 전환할 수 있습니다. 액티브 유닛에서 명령을 입력하는 것이 좋습니다. 그러면 스탠바이 유닛 상태가 재설정됩니다. **show failover** 또는 **show failover state** 명령을 사용하여 유닛의 페일오버 상태를 표시할 수 있습니다.

장애 발생 유닛을 장애 미발생 상태로 복원해도 해당 유닛이 자동으로 액티브 상태로 설정되지 않습니다. 복원된 유닛은 페일오버(강제 또는 자연)를 통해 액티브로 전환될 때까지 스탠바이 상태로 유지됩니다.

디바이스 상태를 재설정해도 디바이스가 장애 발생 상태로 표시된 문제가 해결되지 않습니다. 문제를 해결하지 않거나 모니터링 시간 제한을 늘리지 않으면 디바이스가 장애 발생 상태로 다시 표시될 수 있습니다.

HA 디바이스에서 소프트웨어 업그레이드 설치

네트워크에서 트래픽을 중단하지 않고 고가용성 쌍의 디바이스에서 실행 중인 시스템 소프트웨어를 업그레이드할 수 있습니다. 기본적으로는 액티브 디바이스가 트래픽을 계속 처리하도록 스탠바이 디바이스를 업그레이드합니다. 업그레이드가 완료되고 나면 역할을 전환하여 스탠바이 유닛을 다시 업그레이드합니다.

새시에서 FXOS 버전도 업데이트해야 하는 경우 다음 절차를 사용하여 설치하기 전에 각 디바이스에 FXOS 업그레이드를 설치합니다. 동일한 기술을 사용합니다. FXOS 업그레이드를 대기 디바이스에 설치하고, 역할을 전환하여 대기 디바이스를 활성 상태로 만든 다음 새 (하위 레벨) 대기 디바이스에 업그레이드를 설치합니다.

고가용성 그룹의 유닛이 서로 다른 소프트웨어 버전을 실행하는 동안에는 페일오버가 불가능합니다. 정상적인 상황에서는 유닛이 동일한 소프트웨어 버전을 실행해야 합니다. 유닛이 서로 다른 버전을 실행해도 되는 경우는 소프트웨어 업그레이드를 설치하는 동안뿐입니다.

이 절차에서는 업그레이드 프로세스를 요약하여 설명합니다. 자세한 내용은 [Threat Defense 소프트웨어 업그레이드](#)를 참조하십시오.



참고 업그레이드 시 시스템에서는 시스템 라이브러리를 업데이트(자동 구축 포함)하는 동안 HA를 일시 중단합니다. 이 프로세스의 마지막 부분을 수행하는 동안에는 SSH 연결에 시스템을 사용할 수 있으므로 업그레이드를 적용한 후 바로 로그인하는 경우 HA가 일시 중단된 상태로 표시될 수 있습니다. 시스템이 자체적으로 스탠바이 준비 상태로 돌아가지 않으며 device manager이 사용 가능해지고 자동 구축이 완료된 후에도 이 문제가 계속되면 HA 페이지로 이동하여 HA를 수동으로 다시 시작하십시오.

시작하기 전에

업그레이드 프로세스를 시작하기 전에 액티브 노드에서 보류 중인 변경 사항을 구축해야 합니다. 디바이스를 업그레이드하는 중에는 컨피그레이션을 변경하거나, 한 디바이스를 업그레이드하고 나서 다른 디바이스를 업그레이드하기 전에 구축을 시작하지 마십시오. 이렇게 하지 않으면 구축에서 장애가 발생하며 변경 사항이 손실될 수 있습니다.

대기 모드를 업그레이드한 후에 액티브 유닛에 변경 사항을 구축해야 하는 경우, 액티브 유닛을 업그레이드하기 전에 두 유닛 모두에 해당 구성 변경을 해야 합니다. 그렇지 않으면 하위 레벨 액티브 유닛을 업그레이드한 후 변경 사항을 잃게 됩니다.

작업 목록을 확인하고 실행 중인 작업이 없는지 확인하십시오. 데이터베이스 업데이트 등 모든 작업이 완료될 때까지 대기했다가 업그레이드를 설치하십시오. 예약된 작업도 모두 확인하십시오. 예약 작업이 업그레이드 작업과 중복되지 않게 하십시오.

업데이트를 수행하기 전에 더 이상 사용되지 않는 애플리케이션이 애플리케이션 필터, 액세스 규칙 또는 SSL 암호 해독 규칙에 없는지 확인하십시오. 이러한 애플리케이션의 이름 뒤에는 "(사용되지 않음)"이라고 적혀 있습니다. 이러한 개체에는 더 이상 사용되지 않는 애플리케이션을 추가할 수 없으며, 후속 VDB 업데이트를 수행하면 이전에 유효했던 애플리케이션이 더 이상 사용되지 않게 될 수 있습니다. 이러한 상황이 발생하면 업그레이드에 실패하고 디바이스는 사용할 수 없는 상태가 됩니다.

Cisco 지원 및 다운로드 사이트에서 <https://www.cisco.com/go/ftd-software> 업그레이드 파일을 다운로드합니다.

- 제품군 또는 시리즈의 모든 모델에 동일한 업그레이드 패키지를 사용하십시오. 올바른 버전을 찾으려면 모델을 선택하거나 검색한 다음 해당 버전의 소프트웨어 다운로드 페이지로 이동합니다. 파일 유형이 REL.tar인 적절한 업그레이드 파일을 다운로드해야 합니다. 시스템 소프트웨어 패키지 또는 부트 이미지를 다운로드하지 마십시오.
- 업그레이드 파일의 이름을 바꾸지 마십시오. 이름이 바뀐 파일은 유효하지 않은 것으로 간주됩니다.
- 다운로드하거나 패치를 제거할 수는 없습니다.
- 업그레이드에 필요한 베이스라인 이미지를 실행 중인지 확인합니다. 호환성 정보는 *Cisco Secure Firewall 호환성 가이드* <http://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html>을 참조하십시오.
- 새 버전의 릴리스 노트를 확인합니다. 릴리스 노트는 <http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html>에서 확인할 수 있습니다.

프로시저

단계 1 스텐바이 유닛에 로그인하여 업그레이드를 설치합니다.

- a) **Device**(디바이스)를 선택한 다음 업데이트 요약에서 **View Configuration**(컨피그레이션 보기)을 클릭합니다.
- b) **System Upgrade**(시스템 업그레이드) 그룹에서 **Browse**(찾아보기) 또는 **Upload Another File**(다른 파일 업로드)를 클릭하여 이미지를 업로드합니다.
- c) **Install**(설치)을 클릭하여 설치 프로세스를 시작합니다.

참고 "you must deploy all uncommitted changes before starting a system upgrade(시스템 업그레이드 시작 전에 커밋되지 않은 모든 변경 사항을 구축해야 합니다)" 오류 메시지가 표시되고 활성 유닛에 커밋되지 않은 변경 사항이 없는 경우 활성 유닛에서 약간의 변경 사항을 생성하고 이를 구축합니다. 그런 다음 변경 사항을 취소 할 수 있습니다. 이 방법으로 문제가 해결되지 않고 권장 사항과 일치하지 않는 버전의 HA 그룹을 실행한 경우에는 역할을 전환하여 대기 유닛을 활성 상태로 만든 다음 HA를 일시 중단해야 할 수 있습니다. 그런 다음 활성/일시 중단된 유닛에서 배포하고 HA를 다시 시작한 다음 역할을 전환하여 활성 유닛을 다시 대기 상태로 설정할 수 있습니다. 그러면 업그레이드가 작동합니다.

설치가 완료될 때까지 기다린 후에 다시 로그인하여 시스템이 정상적으로 작동하는지 확인할 수 있습니다.

참고 고가용성 상태를 확인하는 경우 애플리케이션 동기화 실패가 표시될 수 있습니다. 스탠바이 디바이스가 소프트웨어를 업그레이드하는 동안 액티브 디바이스에서 변경 사항을 구축하는 경우에만 이러한 현상이 발생합니다.

단계 2 스탠바이 유닛에서 **Device(디바이스) > High Availability(고가용성)**를 클릭한 다음 기어 메뉴(⚙)에서 **Switch Mode(모드 전환)**를 선택합니다.

이 작업을 수행하면 강제 페일오버가 수행되며 로그인되어 있는 유닛이 액티브 유닛으로 설정됩니다. 유닛 상태가 액티브로 변경될 때까지 기다립니다.

계속 진행하기 전에 선택적으로 네트워크를 테스트하여 디바이스가 연결된 네트워크를 통해 트래픽 플로우가 진행됨을 확인할 수 있습니다.

단계 3 원래 액티브 유닛이었던 새 스탠바이 유닛에 로그인하여 업그레이드를 설치합니다.

해당 프로세스는 위에서 설명한 것과 같습니다. 소프트웨어 업그레이드는 다른 유닛에서 복사되지 않으므로 업로드해야 합니다.

설치가 완료되면 스탠바이 유닛에 다시 로그인하여 설치가 정상적으로 수행되었는지와 유닛이 정상 액티브/스탠바이 상태로 돌아왔는지를 확인합니다. 이 유닛은 자동으로 액티브 상태로 다시 설정되지 않습니다.

참고 고가용성 상태를 확인하는 경우 애플리케이션 동기화 실패가 표시되지 않습니다. 유닛은 이제 동일한 소프트웨어 버전을 실행하므로 액티브 유닛에서 컨피그레이션 가져오기가 성공해야 합니다. 자동 구축에 실패하거나 디바이스가 달리 스탠바이 준비 상태로 전환되지 않는 경우, 기어 메뉴에서 **Resume HA(HA 다시 시작)**를 클릭합니다.

단계 4 현재 액티브 유닛에 로그인합니다. 오류 중인 변경 사항이 있는 경우 구축하고 구축이 정상 완료될 때까지 기다립니다.

단계 5 (선택 사항). 현재 스탠바이 유닛을 다시 액티브 상태로 설정하려면 **Device(디바이스) > High Availability(고가용성)**를 클릭한 다음 두 유닛 중 하나의 기어 메뉴에서 **Switch Mode(모드 전환)**를 선택합니다.

예를 들어 이 프로세스를 시작할 때 기본 유닛이 액티브 유닛이었으며 해당 유닛을 다시 액티브 유닛으로 설정하려는 경우 모드를 전환합니다.

고가용성 쌍의 유닛 교체

필요한 경우에는 네트워크 트래픽을 중단하지 않고 고가용성 그룹에서 유닛을 교체할 수 있습니다.

프로시저

단계 1 교체할 유닛이 작동 중이라면 피어 유닛으로 페일오버를 수행한 다음, 디바이스 CLI에서 **shutdown** 명령을 사용하여 디바이스를 정상적으로 중단해야 합니다. 해당 유닛이 작동하지 않는 경우에는 피어가 액티브 모드로 작동 중인지 확인합니다.

관리자 권한이 있는 경우 **device manager** CLI 콘솔을 통해 **shutdown** 명령을 입력할 수도 있습니다.

단계 2 네트워크에서 유닛을 제거합니다.

단계 3 대체 유닛을 설치하고 인터페이스를 다시 연결합니다.

단계 4 대체 유닛에서 디바이스 설정 마법사를 완료합니다.

단계 5 피어 유닛에서 **High Availability**(고가용성) 페이지로 이동하여 컨피그레이션을 클립보드에 복사합니다. 유닛이 기본 유닛인지 아니면 보조 유닛인지를 확인합니다.

보류 중인 변경 사항이 있으면 지금 구축하고 구축이 완료될 때까지 기다린 후에 계속 진행합니다.

단계 6 대체 유닛에서 **High Availability**(고가용성) 그룹의 **Configure**(구성)를 클릭한 다음 피어에서 반대 유닛 유형을 선택합니다. 즉, 피어가 기본 유닛이면 **Secondary**(보조)를 선택하고 피어가 보조 유닛이면 **Primary**(기본)를 선택합니다.

단계 7 피어에서 HA 컨피그레이션을 붙여넣은 다음 IPsec 키(사용하는 경우)를 입력합니다. **Activate HA**(HA 활성화)를 클릭합니다.

구축이 완료되면 유닛이 피어에 연결하고 HA 그룹에 조인합니다. 이때 액티브 피어의 컨피그레이션을 가져오며, 교체 유닛은 선택한 옵션에 따라 그룹에서 기본 유닛이나 보조 유닛이 됩니다. 이제 HA가 올바르게 작동하는지 확인할 수 있으며 원하는 경우 모드를 전환해 새 유닛을 액티브 유닛으로 설정할 수 있습니다.

고가용성 모니터링

다음 주제에서는 고가용성을 모니터링하는 방법을 설명합니다.

이벤트 뷰어 및 대시보드에는 로그인되어 있는 디바이스와 관련된 데이터만 표시됩니다. 두 디바이스에 대해 병합된 정보는 표시되지 않습니다.

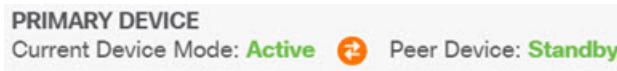
일반 페일오버 상태 및 기록 모니터링

다음과 같은 방법을 사용하여 일반 고가용성 상태 및 기록을 모니터링할 수 있습니다.

- (Device Summary(디바이스 요약)(**Device**(디바이스) 클릭)의 High Availability(고가용성) 그룹에 유닛 상태가 표시됩니다.



- (High Availability(고가용성) 페이지(**Device**(디바이스) > **High Availability**(고가용성) 클릭)에서 두 유닛의 상태를 확인할 수 있습니다. 실패가 발생하면 장애 조치 기록에서 마지막 실패 사유가 표시됩니다. 유닛 사이의 동기화 아이콘을 클릭하면 추가 상태를 확인할 수 있습니다.



- High Availability(고가용성) 페이지에서 상태 옆의 **Failover History**(페일오버 기록) 링크를 클릭합니다. 시스템에서는 CLI 콘솔을 열고 **show failover history details** 명령을 실행합니다. CLI 또는 CLI 콘솔에 직접 이 명령을 입력할 수도 있습니다.

CLI 명령

CLI 또는 CLI에서 콘솔에서 다음 명령을 사용할 수 있습니다.

- **show failover**

유닛의 페일오버 상태에 대한 정보를 표시합니다.

- **show failover history [details]**

이전 페일오버 상태 변경 사항과 상태 변경의 이유가 표시됩니다. 피어 유닛의 페일오버 기록을 표시하려면 **details** 키워드를 추가합니다. 이 정보는 트러블슈팅에 도움이 됩니다.

- **show failover state**

두 유닛의 페일오버 상태가 표시됩니다. 이 정보에는 유닛의 기본/보조 상태, 유닛의 액티브/스탠바이 상태, 마지막으로 보고된 페일오버의 이유가 포함됩니다.

- **show failover statistics**

페일오버 인터페이스의 전송(tx) 및 수신(rx) 패킷 수가 표시됩니다. 예를 들어 유닛이 패킷을 전송은 하지만 수신은 하지 않는 것으로 출력에 표시되는 경우 링크에 문제가 있는 것입니다. 예를 들어 전선이 불량이거나, 피어에 잘못된 IP 주소가 구성되어 있거나, 유닛이 페일오버 인터페이스를 다른 서버넷에 연결하는 등의 문제가 있을 수 있습니다.

```
> show failover statistics
    tx:320875
    rx:0
```

- **show failover interface**

페일오버 및 스테이트풀 페일오버 링크의 컨피그레이션이 표시됩니다. 예를 들면 다음과 같습니다.

```
> show failover interface
  interface failover-link GigabitEthernet1/3
    System IP Address: 192.168.10.1 255.255.255.0
    My IP Address      : 192.168.10.1
    Other IP Address   : 192.168.10.2
  interface stateful-failover-link GigabitEthernet1/4
    System IP Address: 192.168.11.1 255.255.255.0
    My IP Address      : 192.168.11.1
    Other IP Address   : 192.168.11.2
```

- **show monitor-interface**

고가용성을 모니터링하는 인터페이스에 대한 정보가 표시됩니다. 자세한 내용은 [HA 모니터링 인터페이스의 상태 모니터링, 39 페이지](#)를 참조해 주십시오.

- **show running-config failover**

실행 중인 구성의 페일오버 명령을 표시합니다. 이는 고가용성을 구성하는 명령입니다.

HA 모니터링 인터페이스의 상태 모니터링

특정 인터페이스에 대해 HA 모니터링을 활성화한 경우에는 모니터링하는 인터페이스의 상태를 CLI 또는 CLI 콘솔에서 **show monitor-interface** 명령을 사용해 확인할 수 있습니다.

```
> show monitor-interface
This host: Primary - Active
  Interface inside (192.168.1.13): Normal (Monitored)
  Interface outside (192.168.2.13): Normal (Monitored)
Other host: Secondary - Standby Ready
  Interface inside (192.168.1.14): Normal (Monitored)
  Interface outside (192.168.2.14): Normal (Monitored)
```

모니터링한 인터페이스에는 다음과 같은 상태가 표시될 수 있습니다.

- **Unknown (Waiting)**(알 수 없음(대기 중)) 등의 다른 상태와 결합된 **(Waiting)**(대기 중) - 인터페이스가 피어 유닛의 해당 인터페이스에서 hello 패킷을 아직 수신하지 않았습니다.
- **Unknown** - 초기 상태입니다. 이 상태는 상태를 확인할 수 없음을 의미할 수도 있습니다.
- **Normal** - 인터페이스를 트래픽을 받는 중입니다.
- **Testing** - 다섯 번의 폴링 시간 동안 인터페이스에 Hello 메시지가 수신되지 않았습니다.
- **Link Down** - 관리자가 인터페이스 또는 VLAN을 중단했습니다.
- **No Link** - 인터페이스에 대한 물리적 링크가 중단되었습니다.
- **Failed** - 인터페이스에 수신된 트래픽이 없지만 피어 인터페이스에는 트래픽이 수신되었습니다.

HA 관련 Syslog 메시지 모니터링

시스템에서는 심각한 상황을 나타내는 우선순위 레벨 2에 해당하는 페일오버와 관련된 여러 syslog 메시지를 생성합니다. 페일오버와 관련된 메시지 ID의 범위는 101xxx, 102xxx, 103xxx, 104xxx, 105xxx, 210xxx, 311xxx, 709xxx, 727xxx입니다. 예를 들어 105032 및 105043은 페일오버 링크의 문제를 나타냅니다. 시스템 로그 메시지에 대한 설명은 *Cisco Threat Defense Syslog* 메시지 가이드 (https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html)를 참조하십시오.



참고 페일오버가 실행되는 동안에는 시스템에서 인터페이스를 논리적으로 종료했다가 작동시킴으로 syslog 메시지 411001 및 411002가 생성됩니다. 이는 정상적인 동작입니다.

syslog 메시지를 확인하려면 **Device**(디바이스) > **Logging Settings**(로깅 설정)에서 진단 로깅을 구성해야 합니다. 메시지를 안정적으로 모니터링할 수 있도록 외부 syslog 서버를 설정하십시오.

피어 유닛에서 원격으로 CLI 명령 실행

CLI에서는 피어에 로그인할 필요 없이 `failover exec` 명령을 사용하여 피어 디바이스에서 `show` 명령을 입력할 수 있습니다.

failover exec {active | standby | mate} command

명령을 실행해야 하는 유닛(액티브 또는 스탠바이)을 지정하거나, 로그인한 유닛 대신 다른 유닛이 응답하도록 하려는 경우에는 **mate**를 입력해야 합니다.

예를 들어 피어 인터페이스의 컨피그레이션과 통계를 확인하려는 경우 다음 명령을 입력할 수 있습니다.

```
> failover exec mate show interface
```

configure 명령은 입력할 수 없습니다. 이 기능은 **show** 명령과 함께 사용할 수 있습니다.



참고 액티브 유닛에 로그인된 경우에는 **failover reload-standby** 명령을 사용하여 스탠바이 유닛을 다시 로드할 수 있습니다.

device manager CLI 콘솔을 통해 이러한 명령을 입력할 수는 없습니다.

고가용성 트러블슈팅(페일오버)

고가용성 그룹의 유닛이 정상적으로 작동하지 않으면 컨피그레이션 트러블슈팅을 위해 다음 단계 수행을 고려하십시오.

액티브 유닛에 피어 유닛이 Failed(장애 발생)로 표시되는 경우 **유닛의 장애 발생 상태 트러블슈팅, 43 페이지**의 내용을 참조하십시오.

프로시저

단계 1 각 디바이스(기본 및 보조)에서 다음 작업을 수행합니다.

- 다른 디바이스의 IP 주소에 ping을 실행하여 페일오버 링크를 확인합니다.
- 별도의 링크를 사용하는 경우에는 다른 디바이스의 IP 주소에 ping을 실행하여 스테이트풀 페일오버 링크를 확인합니다.

ping에 실패하면 각 디바이스의 인터페이스가 같은 네트워크 세그먼트에 연결되어 있는지 확인합니다. 직접 케이블 연결을 사용하는 경우에는 케이블을 확인합니다.

단계 2 다음과 같은 일반 확인을 수행합니다.

- 기본 디바이스와 보조 디바이스에서 중복 관리 IP 주소를 확인합니다.
- 유닛에서 중복 페일오버 및 스테이트풀 페일오버 IP 주소를 확인합니다.
- 각 디바이스의 동일 인터페이스 포트가 같은 네트워크 세그먼트에 연결되어 있는지 확인합니다.

단계 3 스탠바이 디바이스에서 작업 목록 또는 감사 로그를 확인합니다. 액티브 디바이스에서 모든 구축이 성공하고 나면 "Configuration import from Active node(액티브 노드에서 컨피그레이션 가져오기)" 작업이 성공했음이 표시되어야 합니다. 작업에 실패한 경우 페일오버 링크를 확인하고 구축을 다시 시도합니다.

참고 작업 목록에 실패한 구축 작업이 있었던 것으로 표시되면 구축 작업 중에 장애 조치가 발생한 것일 수 있습니다. 구축 작업을 시작할 때는 스탠바이 디바이스가 액티브 유닛이었다라도 작업 중에 장애 조치가 발생하면 구축에 실패합니다. 이 문제를 해결하려면 모드를 전환하여 스탠바이 유닛을 액티브 유닛으로 다시 설정한 다음, 구성 변경 사항을 다시 구축합니다.

단계 4 **show failover history** 명령을 사용하여 디바이스에서 상태 변경 사항에 대한 세부 정보를 파악합니다.

확인해야 하는 몇 가지 사항은 다음과 같습니다.

- 앱 동기화 실패:

```
12:41:24 UTC Dec 6 2017
```

```
App Sync      Disabled      HA state progression failed due to APP SYNC timeout
```

애플리케이션 동기화 단계에서는 액티브 디바이스의 컨피그레이션이 스탠바이 디바이스로 전송됩니다. 애플리케이션 동기화 실패가 발생하면 디바이스는 비활성화 상태가 되며 더 이상 활성화할 수 없습니다.

디바이스가 앱 동기화 문제로 인해 비활성화되는 경우 페일오버 및 스테이트풀 페일오버 링크의 엔드포인트에 대해 디바이스에서 서로 다른 인터페이스를 사용 중인 것일 수 있습니다. 링크의 양 끝에서 같은 포트 번호를 사용해야 합니다.

`show failover` 명령 실행 시 보조 디바이스가 **Pseudo Standby**(의사 스탠바이) 상태로 표시되는 경우, 해당 상태는 페일오버 링크에 대해 기본 디바이스에서 구성한 것과 다른 IP 주소를 보조 디바이스에서 구성했음을 나타내는 것일 수 있습니다. 페일오버 링크에 대해 두 디바이스에서 같은 기본/보조 IP 주소를 사용 중인지 확인합니다.

Pseudo Standby(의사 스탠바이) 상태는 기본 디바이스와 보조 디바이스에서 서로 다른 IPsec 키를 구성했음을 나타낼 수도 있습니다.

추가 앱 동기화 문제는 [HA 앱 동기화 실패 트러블슈팅, 43 페이지](#)의 내용을 참조하십시오.

- 페일오버가 너무 자주 수행되는 경우(디바이스 상태가 액티브 -> 스탠바이 -> 액티브로 계속 전환됨) 페일오버 링크에 문제가 있는 것일 수 있습니다. 최악의 경우에는 두 유닛이 모두 액티브 상태가 되어 통과 트래픽이 중단될 수도 있습니다. 링크의 양 끝에 대해 ping을 실행하여 연결을 확인합니다. `show arp` 명령을 사용하여 페일오버 IP 주소와 ARP 매핑이 적절한지 확인할 수도 있습니다.

페일오버 링크가 정상 상태이며 정확하게 구성되어 있는 경우에는 피어 폴링 및 대기 시간/인터페이스 폴링 및 대기 시간을 늘리거나, HA를 모니터링하는 인터페이스 수를 줄이거나, 인터페이스 임계값을 늘리는 방법을 고려해 보십시오.

- 인터페이스 확인으로 인한 오류. **Interface Check**(인터페이스 확인) 이유에는 장애가 발생한 것으로 간주된 인터페이스 목록이 포함됩니다. 이러한 인터페이스가 정확하게 구성되어 있으며 하드웨어 문제가 없는지 확인합니다. 링크 반대쪽의 스위치 컨피그레이션에 문제가 없는지 확인합니다. 문제가 없는 경우 해당 인터페이스에서 HA 모니터링 비활성화를 고려해 보십시오. 인터페이스 오류 임계값이나 타이밍을 늘리는 옵션도 있습니다.

06:17:51 UTC Jan 15 2017

Active Failed Interface check

This Host:3

admin: inside

ctx-1: ctx1-1

ctx-2: ctx2-1

Other Host:0

단계 5 스탠바이 유닛을 탐지할 수 없으며 페일오버 링크에서 잘못된 LAN 또는 케이블 연결과 같은 구체적인 이유를 찾을 수 없다면 다음 단계를 시도해 보십시오.

- a) 스탠바이 유닛에서 CLI에 로그인한 다음, **failover reset** 명령을 입력합니다. 이 명령을 실행하면 유닛이 장애 발생 상태에서 장애 미발생 상태로 변경됩니다. 이제 액티브 디바이스에서 HA 상태를 확인합니다. 이제 스탠바이 피어가 탐지되면 작업이 완료된 것입니다.

- b) 액티브 유닛에서 CLI에 로그인한 다음, **failover reset** 명령을 입력합니다. 그러면 액티브 유닛과 스탠바이 유닛 둘 다에서 HA 상태가 재설정됩니다. 디바이스 간의 링크가 재설정되는 것이 가장 좋습니다. HA 상태를 확인하여 아직도 상태가 정확하지 않으면 다음 단계를 계속 진행합니다.
- c) 액티브 디바이스의 CLI 또는 device manager에서 먼저 HA를 일시 중단했다가 다시 시작합니다. CLI 명령은 **configure high-availability suspend** 및 **configure high-availability resume**입니다.
- d) 이러한 단계에서 장애가 발생하면 스탠바이 디바이스를 **reboot**합니다.

유닛의 장애 발생 상태 트러블슈팅

피어 유닛의고가용성 상태(**Device(디바이스)** 또는 **Device(디바이스) > High Availability(고가용성)** 페이지)에서 유닛이 **Failed(장애 발생)**로 표시되는 경우, 유닛 A가 액티브 유닛이고 유닛 B가 장애 발생 피어라고 가정할 때 일반적으로 가능한 원인은 다음과 같습니다.

- 유닛 B가 아직고가용성으로 구성되지 않은 경우(해당 유닛이 아직 독립형 모드임) 유닛 A에 유닛 B가 **Failed(장애 발생)**로 표시됩니다.
- 유닛 B에서 HA를 일시 중단하면 유닛 A에 유닛 B가 **Failed(장애 발생)**로 표시됩니다.
- 유닛 B를 리부팅하는 경우 유닛 B의 리부팅이 완료되고 페일오버 링크를 통한 통신이 다시 시작될 때까지 유닛 A에 유닛 B가 **Failed(장애 발생)**로 표시됩니다.
- 유닛 B에서 애플리케이션 동기화(앱 동기화)에 실패하면 유닛 A에 유닛 B가 **Failed(장애 발생)**로 표시됩니다. [HA 앱 동기화 실패 트러블슈팅, 43 페이지](#)의 내용을 참조하십시오.
- 유닛 B에서 유닛 또는 인터페이스 상태 모니터링에 실패하면 유닛 A에서 유닛 B를 **Failed(장애 발생)**로 표시합니다. 유닛 B에서 시스템 문제를 확인합니다. 디바이스를 리부팅해 봅니다. 유닛이 전반적으로 정상 상태이면 유닛 또는 인터페이스 상태 모니터링 설정 완화를 고려합니다. **show failover history** 출력에서는 인터페이스 상태 확인 실패에 대한 정보를 제공해야 합니다.
- 두 유닛이 모두 액티브 상태가 되면 각 유닛에는 피어가 **Failed(장애 발생)**로 표시됩니다. 이러한 상태는 대개 페일오버 링크의 문제를 나타냅니다.

라이선싱 관련 문제를 표시할 수도 있습니다. 디바이스의 라이선싱은 일관성이 있어야 합니다. 즉 둘 다 평가 모드이거나 등록 상태이어야 합니다. 등록된 경우, 사용하는 스마트 라이선스 계정이 다를 수 있습니다. 하지만 두 계정 모두 내보내기 제어 기능에 대해 동일한 선택을 해야 합니다. 즉 활성화 또는 비활성화 상태여야 합니다. 내보내기 제어 기능에 대한 일관성 없는 설정으로 IPsec 암호화 키를 구성하면 HA를 활성화한 후에 두 디바이스가 모두 활성화됩니다. 이로 인해 지원되는 네트워크 세그먼트에서의 라우팅이 영향을 받게 되고, 이를 복구하기 위해서는 보조 유닛에서 HA를 수동으로 해제해야 합니다.

HA 앱 동기화 실패 트러블슈팅

피어 유닛이 HA 그룹에 조인하지 못하거나 액티브 유닛에서 변경 사항을 구축하는 중에 피어 유닛에서 장애가 발생하는 경우 장애가 발생한 유닛에 로그인하여 **High Availability(고가용성)** 페이지로 이동한 다음 **Failover History(페일오버 기록)** 링크를 클릭합니다. **show failover history** 출력에서 App

Sync(앱 동기화) 실패를 표시하는 경우에는 유닛이 고가용성 그룹으로 정상 작동할 수 있는지를 시스템에서 확인하는 HA 검증 단계에서 문제가 발생한 것입니다.

이러한 유형의 장애는 다음과 같이 표시될 수 있습니다.

```

=====
From State          To State          Reason
=====
16:19:34 UTC May 9 2018
Not Detected       Disabled          No Error

17:08:25 UTC May 9 2018
Disabled          Negotiation      Set by the config command

17:09:10 UTC May 9 2018
Negotiation       Cold Standby     Detected an Active mate

17:09:11 UTC May 9 2018
Cold Standby     App Sync         Detected an Active mate

17:13:07 UTC May 9 2018
App Sync         Disabled          CD App Sync error is
High Availability State Link Interface Mismatch between Primary and Secondary Node

```

문제가 없는 경우에는 From State(시작 상태)가 App Sync(앱 동기화)일 때 "All validation passed(모든 검증 통과)" 메시지를 확인할 수 있으며 노드가 Standby Ready(스탠바이 준비) 상태가 됩니다. 검증 실패 시에는 피어가 Disabled(Failed)(비활성화(장애 발생)) 상태로 전환됩니다. 이 경우 문제를 해결해야 피어가 고가용성 그룹으로 다시 작동합니다. 액티브 유닛을 변경하여 앱 동기화 오류를 해결하는 경우에는 해당 항목을 구축한 다음, 피어 노드가 조인하도록 HA를 다시 시작해야 합니다.

아래에는 장애를 나타내는 메시지와 문제를 해결하는 방법에 대한 설명이 나와 있습니다. 이러한 오류는 노드 조인과 각 후속 구축에서 발생할 수 있습니다. 노드를 조인하는 동안 시스템에서는 액티브 유닛에서 마지막으로 구축된 구성을 확인합니다.

- License registration mode mismatch between Primary and Secondary Node(기본 노드와 보조 노드 간의 라이선스 등록 모드 불일치).

라이선스 오류는 피어 하나는 등록되어 있는데 다른 피어는 평가 모드임을 나타냅니다. 피어는 둘 다 등록되어 있거나 평가 모드여야 HA 그룹에 조인할 수 있습니다. 등록된 디바이스는 평가 모드로 되돌릴 수 없으므로 **Device(디바이스) > Smart License(스마트 라이선스)** 페이지에서 다른 피어를 등록해야 합니다.

등록하는 디바이스가 액티브 유닛이면 디바이스 등록 후에 구축을 수행합니다. 구축을 하면 유닛이 강제로 새로 고쳐지며 컨피그레이션이 동기화됩니다. 그러면 보조 유닛이 고가용성 그룹에 올바르게 조인할 수 있게 됩니다.

- License export compliance mismatch between Primary and Secondary Node(기본 노드와 보조 노드 간의 라이선스 내보내기 컴플라이언스 불일치).

라이선스 컴플라이언스 오류는 두 디바이스가 각기 다른 Cisco Smart Software Manager 어카운트에 등록되어 있는데 내보내기 제어 기능이 어카운트 하나에서는 활성화되어 있고 다른 어카운트에서는 활성화되어 있지 않음을 나타냅니다. 디바이스는 내보내기 제어 기능을 사용하려면

같은 설정(활성화 또는 비활성화)을 사용하는 어카운트에 등록되어 있어야 합니다. **Device**(디바이스) > **Smart License**(스마트 라이선스) 페이지에서 디바이스 등록을 변경합니다.

- **Software version mismatch between Primary and Secondary Node**(기본 노드와 보조 노드 간의 소프트웨어 버전 불일치).

소프트웨어 불일치 오류는 두 피어가 각기 다른 버전의 threat defense 소프트웨어를 실행 중임을 나타냅니다. 소프트웨어 불일치 상태는 소프트웨어 업그레이드를 한 디바이스에 하나씩 설치하는 동안에만 일시적으로 허용됩니다. 그러나 두 피어를 업그레이드하는 시간 사이에는 컨피그레이션 변경 사항을 구축할 수 없습니다. 이 문제를 해결하려면 피어를 업그레이드한 다음 구축을 다시 수행합니다.

- **Physical interfaces mismatch between Primary and Secondary Node**(기본 노드와 보조 노드 간의 물리적 인터페이스 불일치)

HA 그룹의 스탠바이 유닛에는 액티브 유닛에 있는 모든 물리적 인터페이스가 있어야 하며, 이러한 인터페이스의 하드웨어 이름 및 유형(예: GigabitEthernet1/1)은 동일해야 합니다. 이 오류는 액티브 유닛에 있는 일부 인터페이스가 스탠바이 유닛에는 없음을 나타냅니다. 액티브 유닛보다 스탠바이 유닛에 더 많은 인터페이스를 포함할 수 있으므로 액티브 상태인 유닛을 전환하거나 다른 피어 유닛을 선택하십시오. 그러나 예를 들어, 한 유닛에서 인터페이스 모듈을 교체 중이며 해당 유닛을 짧은 시간 동안 모듈 없이 실행해야 하는 경우 일치하지 않는 인터페이스는 임시 상태여야 합니다. 일반적인 작업의 경우에는 두 유닛의 인터페이스 수 및 유형이 동일해야 합니다.

- **Failover link interface mismatch between Primary and Secondary Node**(기본 노드와 보조 노드 간의 페일오버 링크 인터페이스 불일치).

각 유닛의 네트워크에 페일오버 물리적 인터페이스를 연결할 때는 같은 물리적 인터페이스를 선택해야 합니다. 예를 들어 각 유닛에서 GigabitEthernet1/8을 선택합니다. 이 오류는 각기 다른 인터페이스를 사용했음을 나타냅니다. 오류를 해결하려면 피어 유닛에서 케이블링을 수정합니다.

- **Stateful failover link interface mismatch between Primary and Secondary Node**(기본 노드와 보조 노드 간의 스테이트풀 페일오버 링크 인터페이스 불일치).

별도의 스테이트풀 페일오버 링크를 사용하는 경우 각 유닛의 네트워크에 스테이트풀 페일오버 물리적 인터페이스를 연결할 때는 같은 물리적 인터페이스를 선택해야 합니다. 예를 들어 각 유닛에서 GigabitEthernet1/7을 선택합니다. 이 오류는 각기 다른 인터페이스를 사용했음을 나타냅니다. 오류를 해결하려면 피어 유닛에서 케이블링을 수정합니다.

- **Failover/Stateful failover link EtherChannel's member interfaces mismatch between Primary and Secondary Node**(기본 노드와 보조 노드 간의 장애 조치/스테이트풀 장애 조치 링크 EtherChannel 멤버 인터페이스 불일치)

장애 조치 또는 스테이트풀 장애 조치 인터페이스에 대해 EtherChannel 인터페이스를 선택하는 경우, EtherChannel은 각 디바이스에서 ID 및 멤버 인터페이스가 동일해야 합니다. 이 오류 메시지를 통해 불일치가 발생한 곳이 장애 조치인지 스테이트풀 장애 조치 링크인지 알 수 있습니다. 이 오류를 해결하려면 동일한 ID를 사용하고 각 디바이스에 동일한 인터페이스를 포함하도록 EtherChannel 인터페이스의 구성을 수정합니다.

- **Device Model Number mismatch between Primary and Secondary Node**(기본 노드와 보조 노드 간의 디바이스 모델 번호 불일치).

HA 그룹에 조인할 피어는 정확히 동일한 모델의 디바이스여야 합니다. 이 오류는 피어가 동일한 디바이스 모델이 아님을 나타냅니다. HA를 구성하려면 다른 피어를 선택해야 합니다.

- **Active and Standby Nodes cannot be on the same chassis.**(액티브 노드와 스탠바이 노드는 동일한 새시에 있을 수 없습니다.)

동일한 하드웨어 새시에서 호스팅되는 디바이스를 사용하여 고가용성을 구성할 수는 없습니다. 동일한 새시의 여러 디바이스를 지원하는 모델에서 고가용성을 구성하는 경우 별도의 하드웨어에 있는 디바이스를 선택해야 합니다.

- **Unknown error occurred, please try again**(알 수 없는 오류가 발생했습니다. 다시 시도하십시오).

앱 동기화 중에 문제가 발생했는데 시스템에서 문제를 파악할 수 없는 경우입니다. 컨피그레이션 구축을 다시 시도하십시오.

- **Rule package is corrupted. Please update the rule package and try again**(규칙 패키지가 손상되었습니다. 규칙 패키지를 업데이트하고 다시 시도하십시오).

침입 규칙 데이터베이스에 문제가 있습니다. 장애가 발생한 피어에서 **Device**(디바이스) > **Updates**(업데이트)로 이동한 다음 **Rule**(규칙) 그룹에서 **Update Now**(지금 업데이트)를 클릭합니다. 업데이트가 완료될 때까지 기다렸다가 변경 사항을 구축합니다. 그리고 나면 액티브 유닛에서 구축을 재시도할 수 있습니다.

- 클라우드 서비스 등록 상태가 기본 노드와 보조 노드 사이에서 일치하지 않습니다.

노드 중 하나는 Cisco 클라우드에 등록되었지만 다른 노드는 등록되지 않았습니다. 두 노드를 모두 등록해야 하며, 그렇지 않은 경우 등록을 통해 고가용성 그룹을 형성할 수 없습니다. 각 디바이스에서 **Device**(디바이스) > **System Settings**(시스템 설정) > **Cloud Services**(클라우드 서비스)로 이동하고 두 디바이스 모두 동일한 클라우드 서비스 지역에 등록되어 있는지 확인합니다.

- **Active and Standby Nodes cannot have different cloud regions.**(액티브 노드와 스탠바이 노드의 클라우드 지역은 같아야 합니다.)

디바이스가 서로 다른 Cisco Cloud Services 지역에 등록되어 있습니다. 올바른 지역을 확인하고 스마트 라이선싱에서 다른 디바이스를 등록 취소한 다음, 재등록 시 올바른 지역을 선택합니다. 두 디바이스의 지역이 잘못된 경우, 두 디바이스를 모두 등록 취소하고 올바른 지역에 다시 등록합니다.

- **Deployment package is corrupted. Please try again**(구축 패키지가 손상되었습니다. 다시 시도하십시오).

이러한 현상은 시스템 오류입니다. 구축을 다시 시도하면 문제가 해결됩니다.

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.